ＢＳＫ第２４－１号

サイバー空間のための国際戦略

(INTERNATIONAL STRATEGY FOR CYBERSPACE)

― Prosperity,Security,and Openness in a Networked World ―

― ホ　ワ　イ　ト　ハ　ウ　ス　報　告　書 ―

平成２３年１０月

財団法人 防衛調達基盤整備協会

INTERNATIONAL STRATEGY FOR CYBERSPACE

Prosperity, Security, and Openness in a Networked World

MAY 2011

は じ め に

本出版物は、ホワイトハウスが 2011 年 5 月に発表した報告書「サイバー空間のための国際戦略―ネットワーク化された世界の繁栄、セキュリティ、及び公開性（INTERNATIONAL STRATEGY FOR CYBERSPACE－Prosperity, Security, and Openness in a Networked World）を翻訳したものである。

2009 年 1 月に大統領に就任したオバマ大統領は、2010 年５月に「サイバースペース政策の再検討－信頼できかつ弾力性のある情報・通信インフラストラクチャーの確保に向けて（CYBERSPACE POLICY REVIEW－ Assuring a Trusted and Resilient Information and Communications Infrastructure）」（BSK 第 23－2 号）を発表した。本報告書はこれに続く第２弾である。前報告書は、米国内の将来のデジタルインフラの構築に向かう道程が概説されていたが、本報告書では、幅広いサイバーに係る問題に対して、米国は国際的なパートナーと協働して取り組むというアプローチを提示している。「前言」でオバマ大統領は、「今日、国家と国民は、利用できるネットワークに周囲を囲まれている。我々は２つの選択肢を有している。 一つは、我々がより大きな繁栄とセキュリティのために、彼らの可能性を実現するために共に行動することであり、もう一つは、我々が発展を制限する私利私欲と不当な恐れに屈することである」と述べている。

本戦略は、はじめに、サイバー政策を構築する際に、①これまでの成功の上に構築する、②挑戦を認識する、③表現と結社の自由、プライバシー、及び自由な情報の流れの 3 つの原則を土台にする、という戦略的アプローチを概説している。次に、①公開性と相互運用性、②セキュリティと信頼性、及び③規範を通しての安定性、が我々の求めるサイバー空間の将来像であり、それを実現するために果たすべき外交、防衛、及びセキュリティ上の役割等が概説されている。そして最後に、国内外の米国のパートナーが米国のサイバー政策の優先事項を理解するために必要な背景等が概説されている。

サイバー犯罪のグローバル化について、警察白書（平成 22 年版 ）は、「インターネットは、日本国内のみにとどまるものではなく、海外にも広がっていることから、海外からの不正アクセス行為等の国境を越えたサイバー犯罪が発生している。平成 21 年中の海外からの不正アクセス行為の認知件数は 40 件としていた。それが同白書 23 年版では、平成 22 年の不正アクセスは 1,755 件と急増ぶりを示している。このようにサイバー攻撃のグローバル化は、我が国においても重要な課題となっている。

本小冊子が、我が国の情報セキュリティ体制の向上にいささかでも貢献できれば望外の幸せである。

平成 23 年 10 月

財団法人　防衛調達基盤整備協会
理事長　宇 田 川　 新 一

サイバー空間のための国際戦路

ネットワーク化された世界の繁栄、セキュリティ、及び開放性

2011 年 5 月

ホワイトハウス

ワシントン

サイバー空間は、あらゆる国籍、人種、信仰、及び考え方の人々が、これまでにない方法で情報を交換し、協力し、繁栄することを可能とする。それを可能としているのは技術である。今日、米国企業はインターネット接続により世界中でビジネスを行うことができる。そして、無数の仕事と機会を米国の人々に提供している。アフリカの田舎に住む母親が、中南米の家族に工芸品を売ることができる。それは、より広範な経済発展を促進する。ヨーロッパの研究所は、アジアで作られたハードウェアと北アメリカで書かれたソフトウェアを使って新しい研究を実施することができる。オーストラリアと中東の学生は、ビデオ講義を通して一緒に学ぶことができる。また、世界中の人々は、情報技術によって、かつてないほど彼らの政府の公開性と国民の要求への応答性を高める力を得た。

今日、国家と国民は、利用できるネットワークに周囲を囲まれている。我々は２つの選択肢を有している。 一つは、我々がより大きな繁栄とセキュリティのために、彼らの可能性を実現するために共に行動することであり、もう一つは、我々が発展を制限する私利私欲と不当な恐れに屈することである。サイバーセキュリティは、それ自体が目的ではない。それは、イノベーションを起こし続け、市場を活性化し、そして、生活を改善することを確実にするために、我々の政府と社会が積極的に責任を引き受けなければならない義務である。オフラインの犯罪と侵害がデジタル世界に蔓延してきたが、我々は、我々が大切にしている原則に従い、これに立ち向かうであろう。その原則とは、表現と結社の自由、プライバシー、及び自由な情報の流れである。

デジタル世界は、もはや不法な未開拓分野でも、小さなエリート集団だけの領域でもない。そこは、利用し始めた国家と人々によって実行される責任、公正、及び平和の規範が存在する場所である。その効果的な管理を確実にするためには、市民社会、学界、民間セクター、及び政府が、民主的に協働することが組織化されているコミュニティが、理想である。最も重要なことは、このサイバー空間は、その発明以来、成長と発達をし続け、さらに繁栄、セキュリティ、及び公開性を促進している。これが、インターネットを国際的な環境の中で保護することが重要である理由である。

この精神で、私（オバマ大統領）は、サイバー空間のための国際戦略を提示する。私の政権がこれらの技術を取巻く課題に取り組むのは初めてではないが、幅広いサイバー問題に、我が国と国際的なパートナーが一体となって取り組むというアプローチを提示したのは今回が初めてである。従って、本戦略は、サイバー空間の将来の展望だけでなく、それを実現するための課題を概説している。本戦略は、国内外の我々のパートナーが我々の優先事項を理解するための背景とサイバー空間の特質を維持しながら我々が直面する脅威を減少させるために我々が協力して何ができるかを示している。

インターネットそれ自身は、国際協力の新しい時代の到来を告げるものではない。その仕事が達成できるかどうかは、その受益者である我々次第である。我々は、公開性、相互運用性、セキュリティ、及び信頼性のあるサイバー空間の将来を構築するために協力することができる。これが、我々が求める将来である。我々は、すべての国々及び人々に、この努力に我々と共に参加するよう呼びかける。

バラク・オバマ大統領

目　次

第１章　サイバー空間政策の構築 ・・・・・・・・・・・・・・・・・・・・・・・・・ １
１．戦略的アプローチ　・・・・・・・・・・・・・・・・・・・・・・・・・・・・ ２
（１）成功の上に構築する。　・・・・・・・・・・・・・・・・・・・・・・・・ ２
（２）挑戦を認識する。　・・・・・・・・・・・・・・・・・・・・・・・・・・ ３
（３）原則を土台にする。　・・・・・・・・・・・・・・・・・・・・・・・・・ ３

第２章　サイバー空間の将来３ ・・・・・・・・・・・・・・・・・・・・・・・・・６
１．我々が求める将来　３ ・・・・・・・・・・・・・・・・・・・・・・・・・・７
（１）開放性と相互運用性：力を与えるサイバー空間　・・・・・・・・・・・・・７
（２）セキュリティと信頼性：持続するサイバー空間　・・・・・・・・・・・・・８
（３）規範を通しての安定性　・・・・・・・・・・・・・・・・・・・・・・・・９
２．サイバー空間の将来における我々の役割　・・・・・・・・・・・・・・・・・１１
（１）外交：パートナーシップの強化　・・・・・・・・・・・・・・・・・・・・１１
（２）防衛：拒否的抑止と制裁的抑止　・・・・・・・・・・・・・・・・・・・・１３
（３）開発：繁栄とセキュリティの構築　・・・・・・・・・・・・・・・・・・・１５

第３章　政策の優先事項 ・・・・・・・・・・・・・・・・・・・・・・・・・・・１８
１．経済：国際標準、イノベーション、及び「開かれた市場」の促進　・・・・・１８
２．我々のネットワークの防護：セキュリティ、信頼性、及び弾力性の強化　・・１９
３．法執行：協働と「法の支配」の拡大　・・・・・・・・・・・・・・・・・・・２１
４．軍事：21 世紀の安全保障上の課題への備え　・・・・・・・・・・・・・・・２２
５．インターネット・ガバナンス：効果的で誰にでも受け入れやすい構造の促進　２３
６．国際的な開発：能力、セキュリティ、及び繁栄の構築　・・・・・・・・・・２４
７．インターネット自由：基本的自由とプライバシーの支持　・・・・・・・・・２６

第４章　将来へ向かっての前進 ・・・・・・・・・・・・・・・・・・・・・・・・２８

第１章　サイバー空間政策の構築

“我々は、このサイバー空間の世界に、一日も欠かさず依存している。我々は、サイバー空間によって、人間の歴史の中で今が最も相互接続されている。"
バラク・オバマ大統領、2009 年 5 月 29 目

デジタル基盤は、ますます経済の繁栄、研究コミュニティの活性化、軍隊の強大化、政府の透明性、及び社会の自由化の重要な要素となっている。かつてないほど、情報技術は国境を越えた対話を促進し、商品とサービスの世界的な流れを容易にしている。これらの社会的及び商業上の結びつきは、我々の目常生活にとって不可欠なものになった。電気と水を供給する最重要な生命維持インフラ、航空交通の管制、及び金融システムのすべてがネットワーク化された情報システムに依存している。政府は、現在、電子政府のイニシアティブを通して重要なサービスの提供を合理化することができる。社会的及び政治的活動は、組織と行動を新しくかつより広範な活動にするためにインターネットに依存している。ネットワーク化技術により世界中が接続されている。すべての国にとって、デジタル基盤は、国家資産になっているか又はなりつつある。

ネットワーク化技術が世界に約束した恩恵を実現するためには、これらのシステムは信頼性とセキュリティを有していなければならない。人々は、データが混乱なくその目的地に到達することに自信がなければならない。情報の自由な流れ、セキュリティ、プライバシー、及び相互接続したネットワーク自体の完全性を確保することは、米国と世界の経済の繁栄、安全保障、及び普遍的な価値の促進にとって必須である。

世界の人口のほぼ 3 分の 1 は、インターネットを使用し、それ以上の数えきれない人々が毎日の生活の中でインターネットに触れている。今日、世界には 40 億のデジタル無線装置がある。わずか半世紀前には、その数はゼロであった。我々は、これまでのサイバー空間の成功を土台に前進し、そして、米国国民とグローバルコミュニティのサイバー空間の将来をセキュアにすることのできるまれな歴史の瞬間に生きている。

個人に力を与え、社会を豊かにし、そして、近代的な経済を構築するために不可欠な研究・開発・イノベーションを促進し続けるために、サイバー空間は、その爆発的な成長を特徴づけた開放性と相互運用性を保持し続けなければならない。これの基礎となるものは技術的な原則と効果的な統治構造である。そして、それらは、我々の支援を必要としている。同時に、我々のネットワークはセキュアで信頼できなければならない。ネットワークは、個人、企業、及び政府の信用を保持しなければならならない。そして、恣意的又は悪意の

ある混乱に対する弾力性がなければならない。

世界は、サイバー空間へ侵入しようとする悪意のあるアクターによってもたらされる挑戦を共に認識し、それに対応して、我々の国家政策と国際政策を更新・強化しなければならない。サイバー空間で行われる活動は、物理的空間における我々の生活にも影響がある。サイバー空間を利用する利益を上回るリスクを防止するために、我々は法の支配の構築を目指し努力しなければならない。我々は、ますますネットワーク化された世界を不安定にするか又は弱体化しようとする悪意ある人々に立ち向かうが、一方で将来のサイバー空間の公開性、相互運用性、セキュリティ、及び信頼性は、我々が国家としそれらを認識・保護することにかかっている。

１．戦略的アプローチ

米国の国際サイバー空間政策の根拠は、ネットワーク化技術が、我が国（米国)、そして世界に計り知れない可能性を持っているという確信である。この 30 年の間、我々は、これらの技術が我々の経済に革命をもたらし、我々の目常生活に変革をもたらすのを目の当たりにしてきた。我々はまた、情報窃盗や攻撃などの挑戦がサイバー空間へ移動するのを目撃した。我々は、それらの挑戦に順応することにより、世界の国々に模範を示し先導する。米国は、経済をけん引するイノベーションを引き起こし、国内外の生活を改善する国際サイバー空間政策を遂行する。これらの努力のすべてにおいて、我々は、米国の外交政策でなく、インターネットそのものの将来にとって重要な原則を土台としている。

(1)成功の上に構築する。

米国は、我々の社会と経済におけるデジタルネットワークの恩恵を保護・強化することを公約している。

これらの恩恵は多様かつ広範囲である。個人のために、コンピュータ・ネットワークは生産性と繁栄を強化した。また、コンピュータ・ネットワークは、不利な立場や障害を克服するのを助け、言語又は稀有な病気によって孤立した人々を引き合わせ、そして国境から遠く離れた家族や友人を結びつけた。コミュニティのために、コンピュータ・ネットワークは、緊急事態への初期対応を迅速にし、犯罪解決のための情報共有を拡大し、政治的腐敗に光を投げ掛け、政治的行動を容易にし、そして、見落とされた原因に対して多くの人々の注意を向けさせた。企業のために、コンピュータ・ネットワークは、新しい市場を開き、10 億ドルの産業を生み出した。政府のために、コンピュータ・ネットワークは、透明性、

効率性、及び便利さを可能にするとともに、リーダーと市民とを結びつけた。国際社会のために、コンピュータ・ネットワークは、アイデアを交換し合うグローバルな市場の基礎を提供し、あるいは大規模な災害時に驚くべき寄付を集めるのを手助けした。情報の流れがより自由であれば、我々の社会は、より強固になる。適切に使用されれば、これらの技術は我々すべてを強化することができる。我々はこれらの技術の使用範囲の拡大と国内外における運用の改善に努力する。

(2) 挑戦を認識する。

米国は、これらのネットワークの成長が我々の国家及び経済安全保障並びにグローバルコミュニティの安全保障に対する新しい挑戦をもたらしていることを認識している。

これらの挑戦は、様々な形で現れる。天災、事故、又は破壊活動は、国内外のケーブル、サーバー、及び無線ネットワークを中断させることができる。ある国のウェブサイトを妨害する方法は、滝のように他の国々に拡散するように技術的な挑戦は破壊的である。恐喝、詐欺、個人情報の窃盗、及び児童(の性的)搾取は、電子商取引、ソーシャル・ネットワークを使用するユーザーの信頼を脅かし、さらに彼らの個人的安全さえも脅かす。知的所有権の窃盗は、それを保有する国家の競争力とイノベーションを脅かす。これらの挑戦は、国境を越えて拡大する。サイバー空間への侵入の容易さと匿名性による仮想実在（virtual presence）を構築する能力は、国家が認識しているいないにかかわらず、犯人の「安全避難所（safe havens)」に繋がっている。従来の対立の形がサイバー空間に拡大したことにより、サイバーセキュリティの脅威は、より広範に国際社会の平和と安全保障を危険にさらしている。

(3)原則を土台にする。

米国は、我々にとって重要な原則を守りながらこれらの挑戦に立ち向かっている。

我々の政策は、公約からさらに進んで、サイバー空間を最良の状態に維持すること及び我々の原則を守ることへと移行している。我々のサイバー空間のための国際政策は、基本的自由、プライバシー、及び「情報の自由な流れ」に対する我々の重要な公約を反映している。

①基本的自由：表現と結社の自由に関する我々の公約は、順守されなければならないが、治安あるいは市民の保護を犠牲にしては成り立たない。国際的に「基本的自由」として認められたこれらの人権の中で、情報とアイデアを探し求め、受け取り、開示する能力は、いかなる媒体を通じようとあるいは国境を越えようと、今までは全く問題とならなかった。

我々は、悪意を持ったインターネットユーザーがいることを知っている。サイバー空間の表現の自由に対する制限は、最小限かつ必要性に応じたものでなければならない。また、例えば、児童ポルノ、差し迫った暴力の教唆、又はテロリズムの行為の組織化は、どんな社会においても受け入れられない。それらはインターネット上に存在する余地はない。米国は、インターネットの価値について社会に問うのではなく、我々の中心的な価値と一致する方法で問題を具体的に処理しながら彼らと戦い続ける。

②プライバシー：我々の戦略は、市民を保護する我々の義務とプライバシーに対する我々の公約と一致する。市民は、彼らの公的及び私的生活の中でますますインターネットを使用するようになっている。そのため個人は、彼らの個人データがどのように使用されているかを理解し、そして、それが公正に取り扱われると確信できなければならない。同様に、市民は、インターネットに潜んでいる詐欺、窃盗、及び脅迫から個人的安全まで保護されていると思っている。また、市民は、他人を侵害するためにインターネットを使用している人々を捜査・起訴するために、法執行機関が法律に従い自由にすべてのツールを使用していると思っている。米国は、法執行機関にそれが必要とする適切な捜査権限を与える一方で、法の支配との一貫性を確実にするために適切な司法審査と監視を通して個人の権利を保護することにより、この方程式のバランスを確保することを確約する。

③情報の自由な流れ：国家は、情報の自由な流れとネットワークのセキュリティのどちらかを選ぶ必要がなく、また、選ぶべきではない。サイバーセキュリティの最善の解決策とは、ネットワーク・パフォーマンスへの影響が最少で、ダイナミックかつ適応性があるものである。これらのツールは、イノベーションを鈍らせず、表現や結社の自由を抑圧せず、あるいはグローバルな相互運用性を妨げることなく、システムのセキュリティを確保する。これとは対照的に、我々は、国家レベルのフィルターとファイアーウォールによるアプローチを目の当たりにしている。それはセキュリティが確保されているという幻想を与える一方で、開放性、相互運用性、セキュリティ、及び信頼性を持った情報交換の媒体としてのインターネットの効果と成長を妨げている。同じことが、商業にも当てはまる。サイバー空間は、イノベーション、企業家精神、勤勉さに報いる公平な競争の場のままでなければならず、国家が不当な有利さを得るために情報の自由な流れを恣意的に中断させる場であってはならない。米国は、我々の国家ニーズだけでなく世界的な責任を認識しつつ、自由貿易と情報のより広範な自由の流れを保護する一方で、サイバーセキュリティを強化する国際的なイニシアティブと標準化に努力することを確約する。

以上の原則は、しばしば効果的な法執行、匿名性、子供の保護、及びセキュアなインフラと相いれないと見なされる。しかし、実際には、優れたサイバーセキュリティはプライバシーを強化し、また、違法な行動を標的とした効果的な法執行は基本的自由を保護するこ

とができる。法の支配(法律に対する忠誠心が人々と利益を保護する社会の秩序)は、世界市場に安定をもたらし、悪意あるアクターの責任を国際的に問うことができる。そして世界市場の安定と悪意あるアクターの排除は、我々の国家安全保障を支え、我々の共通の価値を促進する。

第 2 章　サイバー空間の将来

企業や一般家庭が利用できる価格で、インターネットへの信頼できるアクセスが地球上のどこからも可能である将来を想像してください。コンピュータは、近所あるいは世界中の友人や同僚との信頼できる瞬時の相互通信を、シームレスかつグローバルなネットワークによって可能とする。コンテンツは、現地語で提供され国境を越えて自由に流れている。そしてデジタル翻訳の改善により、豊かな知識、新しいアイデア、及び有意義な議論が数百万の人々に公開されている。農業の改善や公衆衛生の向上に関連する技術は、それらを必要とする人々と共有され、困難な問題については、専門家や発明家との間で世界的な協力が行われている。これが、米国が求めるサイバー空間の将来の一つの姿であり、我々が実現しようとする将来である。

このような将来では、個人や企業は、オンラインで使用するために必要なツールを迅速かつ容易に入手することができる。面倒な許可又は個人情報の不合理な開示なしで、ドメイン名とアドレスはすぐに使用でき、ネットワークはセキュアで、かつ適切に管理されている。優秀なエンジニア達は、ネットワークをより速く、より信頼できるようにするために、情報システムの新しい基準の開発について国際的に協力する。そして、イノベーションに対して触媒作用を及ぼすとともに、アクセスのし易さを拡大する。ハイテク企業は、よりセキュアで、より信頼でき、かつ顧客のニーズにより対応したソフトウェア、ハードウェア、及びサービスを提供するために顧客と協力する。

将来、大学と企業は、新しいコンセプトと製品を自由に研究・開発することができる。何故ならば、彼らは、彼らの知的所有権と共有ネットワーク上の価値あるデータが安全であることを理解しているからである。個人は、彼らのパソコンに対する脅威を認識し、彼らのシステムを保護するために簡便な措置をとることができる。民間企業は、彼らのネットワークのウイルス対策に責任を負う。彼らは、そうすることによって彼らの投資を保護することができる。政府は、サイバー・セキュリティ・インシデントの措置を必要とする時、早期にそれらの脅威を探知し、マルウエアの拡大を局限し、大規模な混乱による影響を最小限にするためにリアルタイムでデータを共有することができる。その間中、一般的な情報の自由な流れは保護される。国際的な犯罪が行われたときには、各国の法執行機関は証拠を保護・共有して、犯人を起訴するために協力する。

このような将来は、より大きな繁栄とより信頼できるネットワークだけでなく、強化された国際的な安全保障とより持続的な平和を約束する。その中で、各国は、混乱を回避する方法でネットワークを設定するか又は犯人が安全な避難場所からインターネットを使用す

るのを阻止するために責任ある当事者として行動する。各国は、ネットワーク化されたインフラが防護されていなければならないということを知っており、それを混乱と破壊活動から防護するための措置を講じている。各国は、世界のより多くの国を情報化社会に参入させるため及びインターネットとその重要な特性を保護するというコンセンサスに参加させるために、二国間、多国間、及び国際的枠組みでの協力を継続している。

米国と増え続けるパートナーは、すでに将来のための基礎を築いた。しかし、サイバー空間の将来は予測できない。そして我々は単独でそれを築くことはできない。進展は遅く、資源集約的であるかもしれないが、国際社会は、長期的な投資を継続するために協力しなければならない。我々は、サイバー空間に関するこの展望が、国際社会の共通した目的と同じくらい国益にも役立つことを明白に理解した上で取り組まなければならない。我々の成功には、これまでの半世紀の移行期と同様にさらに半世紀が必要であろう。これまでの半世紀で、我々は、恩恵を完全に理解し、グローバルな相互接続のリスクを最小化した。

1. 我々が求める将来

我々が求めるサイバー空間環境は、イノベーションに報い、個人の力になるものである。それは個人同士をつなぎ、コミュニティを強化する。それはより良い政府を築き、説明責任を拡大する。それは基本的自由を保護し、個人のプライバシーを強化する。それは理解を深め、行動の規範を明確にする。そして、それは国家と国際社会の安全保障を強化する。この環境を支えるための国際社会の協働は、ベストプラクティス以上のものである。これは自明のことである。

我々の目標

米国は、情報・通信インフラの開放性、相互運用性、セキュリティ、及び信頼性を促進するために、国際社会と協力する。それは、国際貿易と商業を支援し、国際社会の安全保障を強化し、そして表現の自由とイノベーションを促進する。その目標を達成するために、我々は責任ある行動規範が国家の行動を導く環境を構築・維持し、パートナーシップを継続し、そして、サイバー空間における法の支配を支持する。

(1) 開放性と相互運用性：力を与えるサイバー空間

デジタル・イノベーションの核心は、ネットワーク化されたマシンに新しい機能性を与える能力である。デジタルシステムは、開放性によって、爆発的な成長と急速な発展をし、そして揺るぎない重要性を獲得した。コンピュータのインターネット接続があらゆる国に拡大するのに伴い、ネットワーク化技術の基本的ツールの有用性は着実に増加し、価格は

減少している。絶えず増加するインターネット利用者のニーズを満足し続けるために、ハードウェアとオペレーティング・システムのメーカーは、世界中のできるだけ広範な開発者に力を与え続けなければならない。企業が独占所有権のあるソフトウェアの開発でイノベーションを目指す一方で、我々はオープンソースソフトウェア開発に拍手を送る。こうすることにより、開発者と消費者に、彼らのニーズを満足するコミュニティ主体の解決策を選択する機会を与えることができる。

米国は、エンドツーエンドの相互運用性を持ったインターネットを支持する。それは、世界中の人々が、彼らのニーズを満たす技術によってお互いを接続し知識や考え方を共有することを可能にする。情報の自由な流れは、国連世界情報社会サミット(World Summit on the Information Society : WSIS)のチュニス・コミットメントにおいて 174 の国によって賛同された原則、即ち相互運用性に依存している。地球規模の開放性と相互運用性がなければ、インターネットは小間切れとなる。そして、少数の国々の政治的利益のために、世界の人口の多くが、高度なアプリケーションと豊富なコンテンツへのアクセスが拒否されるであろう。情報通信技術の国際標準のコンセンサス・ベースの協働開発は、開放性と相互運用性を保持しながら、我々のデジタル経済を拡大し、我々の社会を前進させるための重要な要素である。

(2) セキュリティと信頼性：持続するサイバー空間

持続するサイバー空間であるためには、我々のネットワーク化されたシステムは、まず我々の信頼を保持しなければならない。ユーザーは、送られてきたデータが信頼できることと同様に、彼らのデータがセキュアに送信かつ保管されることに自信を持つ必要がある。効果的な戦略には、社会のあらゆるレベルでの責任の共有と、下はエンドユーザーから上は国家間の協働まで、多くの正面での行動が必要である。脆弱性の縮小には、強固な技術的基準及び解決法、効果的なインシデント管理、信頼できるハードウェア及びソフトウェア、並びにセキュアなサプライチェーンが必要である。地球規模のリスク削減には、国際的に同意された国家行動に関する規範、信頼を構築し透明性を高める措置、積極的かつ情報に基づいた外交、及び適切な抑止などの効果的な法執行が必要である。最後に、インシデント対応には、民間セクターと国際社会とのさらなる協働と技術的な情報共有が必要である。いかなる国あるいはセクターであっても、単独では、この作業に取り組むことはできない。あらゆる国と人々すべてが共有する責任と義務が不可欠である。ネットワークの安定性は、我々のグローバルな繁栄の土台である。そして、ネットワークのセキュリティを確保することは厳密に言えば技術的な問題以上のものである。経済的に言えば、国内外のインフラに投資し、持続的に発展させなければならない。その一方で、ネットワークの信頼性向上を奨励し、そのための企業と国家の義務を明確にしなければならない。政治的には、我々

はサイバー空間を尊重する環境を維持することを支援しなければならない。そうすれば、対立・紛争はネットワークを混乱・劣化させる理由にならなくなるであろう。社会的には、我々は、エンドユーザーに、彼らの装置を安全かつセキュアな方法で維持・運用するという彼らの責任を気づかせなければならない。

(3) 規範を通しての安定性

米国は、期待される環境又は行動規範を構築するために、同じ考えを持った国々と協力する。それは外交及び防衛政策の基礎となり、国際的パートナーシップを促進する。この 20 年の間に、インターネットは社会的な媒体として急速かつ先例のない成長をなしとげた。社会は、現代生活にとって必須の重要インフラ及び通信システムを制御するネットワーク化された情報システムへの依存を増大し続けた。そして、政府がサイバー空間を介して伝統的な国力を作用させようとしている証拠が増加している。このような事象は、サイバー空間で許容される国家の行動についてこれまでに合意された規範とは明らかに一致しない。このギャップを埋めるために、我々は、許容できる行動とは何かについてのコンセンサスの構築、及びこれらのシステムを機能させることが国益及び集団的な利益に不可欠であると考える国々との間のパートナーシップの構築に努力する。

ア．規範の役割

国際関係の他の領域では、許容される行動に関する共通した理解は、安定性を強化するとともに、集団的な措置が必要な場合に国際的な行動の基礎を提供した。そのような規範の順守は、国家の行動に関する予測性をもたらすとともに対立につながる誤解の防止に役立つものである。

サイバー空間にかかわる国家の行動に関する規範の開発は、国際慣習法の再策定を必要としないし、既存の国際的規範も陳腐化しない。長期にわたり平和及び紛争時の国家の行動を導いてきた規範は、サイバー空間にも適用できる。とはいえ、ネットワーク化技術の独特の性質は、これらの規範がどのように適用されるのか、どんなさらなる了解事項が必要になるか、を明確するための更なる作業を必要とする。我々は、いかに行動規範をサイバー空間に適用するかに関するコンセンサスを作るための国際的な努力を継続する。そして、そのような努力の重要な第一歩は、サイバー空間にかかわる平和で公平な国家間の行動に向けられるであろう。

イ．規範のための土台

秩序と平和を促進する、基本的な人間の尊厳を促進する、そして、経済競争における自由を促進するというルールは、どんな国際環境にとっても必須である。これらの原則は、国

家がサイバー空間において彼らの伝統的な国際的義務を果たす際の基本的な指針を提供する。そして、多くの場合、これらの原則は、状況に関係なく適用される国家の義務を反映している。

①基本的自由(Fundamental Freedoms)の支持：国家は、オフラインと同様にオンラインにおいても、表現と結社の基本的自由を尊重しなければならない。

②所有権の尊重：国家は、国内法を通して、業務上の特許、企業秘密、商標、及び著作権を含む知的所有権を尊重しなければならない。

③プライバシーの尊重：個人は、彼らがインターネットを使用しているとき、彼らのプライバシーへの恣意的又は違法な国家の干渉から保護されなければならない。

④犯罪からの保護：国家は、法律と捜査により犯人に安全な避難所(safe havens)を与えないために、サイバー犯罪人を特定し、起訴しなければならない。そして、国際的な犯罪捜査機関とタイムリーに協力しなければならない。

⑤自衛権（Right of Self - defense）：国連憲章に基づき、国家は、サイバー空間におけるある種の攻撃的行為に対する固有の自衛権を有している。

国家間の行動に関するこれらの伝統的な原則に由来する責任は、サイバー空間ではより具体的である。とりわけ、地球規模のネットワークの機能性を維持し、サイバーセキュリティを改善することが重視される。これらの責任の多くは、インターネットの技術的な性質に根差している。インターネットの中核的機能は、例えばボーダ・ゲートウェイ・プロトコル(BGP)のようなシステムの信頼性に依存しているので、国家はそれらの技術的取決めの国際的な関連を認識し、お互いのネットワークとより広範なインターネットを尊重して行動する必要がある。同様に、これらのシステムの次世代を設計する際には、単に国家の威信又は政治的支配を強化することより、むしろ最も健全な技術基準と統治構造を支持することにより、我々は共通の利益を推進しなければならない。また、以下の新しい規範もサイバー空間に必須のものである。

⑥グローバルな相互運用性：国家は、すべての人々がアクセスできるインターネットのエンドツーエンドの相互運用性を確保するために、国家の権限内で行動すべきである。

⑦ネットワークの安定性：国家は、自国のネットワーク構造内での情報の自由な流れを尊重しなければならない。そして、国家は、国際的に相互接続したインフラに対して恣意的な干渉を行わないことを保証する。

⑧確実なアクセス：国家は、インターネット又は他のネットワーク化された技術に対する個人のアクセスを恣意的に奪ったり又は中断させてはいけない。

⑨複数利害関係者による統治：インターネット・ガバナンスのための努力には、政府に限定せず、すべての適切な利害関係者が含まれなければならない。

⑩サイバーセキュリティへの十分な配慮：国家は、情報インフラを防護し、損傷又は不正使用から国家システムを保全するという彼らの責任を認識し、行動しなければならない。

サイバー空間はダイナミックな環境であるが、そこにおける国際的な行動は、信頼できる国内の統治、平和的な国家間の処理、及び信頼できるネットワーク管理の原則に基づいていなければならない。これらの考えが発展するにつれて、米国はこの考えを支持し、議論に積極的に参加する。そして、インターネット政策立案の際の原則基盤アプローチ（principled approach）を促進するとともに、其々の問題に適したフォーラムにおいて共通の理解を促進する。

２．サイバー空間の将来における我々の役割

建設的な規範を普及し、我々の考える将来を実現するために、米国は、外交、防衛、及び開発の３つのアプローチを結合し、すべての人々がネットワーク化技術の恩恵を享受できるよう、繁栄、セキュリティ、及び開放性を強化する。これらの 3 つのアプローチは、我々の国際的努力の中心である。20 世紀の後半、米国は国際的な経済と安全保障の新しい戦後体制の構築を支援した。21 世紀には、我々は、これと同じ協力と連帯の精神で、平和で信頼できるサイバー空間を実現する。

(1) 外交：パートナーシップの強化

サイバー空間の恩恵と特質を維持しながら、平和と安全保障の原則をサイバー空間へ拡大するには、強固なパートナーシップと拡大されたイニシアティブが必要である。我々は、サイバー空間システムの安定性を強化するために、国際社会との対話を率直かつ至急に行い、サイバー空間に関する責任ある行動の原則と必要な措置について国内と国際社会双方でのコンセンサスを構築する。

外交目標

米国は、開放性、相互運用性、セキュリティ、及び信頼性のあるサイバー空間の固有の価値を認識している国々が協力し、責任ある利害関係者として行動する国際環境に関するコンセンサスを構築するために努力する。必要に応じて奨励措置を講ずる。

我々の国際的な友好・協力関係を通して、我々は、まさに、できるだけ多くの利害関係者がサイバー空間に関するコンセンサスの構築に参加することを促進している。何故ならば、これは、経済的、社会的、政治的、及び安全保障上の利益を促進するからである。これらの努力は国内外の民間セクターとの有意義な協働によって支えられる。

分散処理システムでは、分散された措置が必要である。一つの機関、文書、協定、又は指示書では、我々のネットワーク化された世界のニーズに対処するには十分でない。エンドユーザー、民間セクターのハードウェアとソフトウェアのベンダー、及びインターネット・サービス・プロバイダ(ISP)から、地域、多国間、及び複数利害関係者（Multi - stakeholder）の組織までのすべてが、サイバー空間のすべての可能性を実現するための重要な要素である。

①二国間及び多国間のパートナーシップ：我々は、我々の政府と国民にとって重要なサイバー空間の問題について各国と二国間の協議を行う。サイバー空間の行動規範について広範な国際的理解を構築するためには、同じ考えを持った国々との明確な合意作りから始めなければならない。我々は、これらの努力を推進するために広範な仲間からなる共同体を求めている。そして、我々は、あらゆるレベルの二国間対話にサイバー空間に関する問題を組み込んでいる。我々は、すでに成功しているツールと方法を実行しながら、サイバー空間の新しい挑戦に対処する共通の行動を促進する。さらに、我々は発展途上の国々に積極的に呼びかけ、これらの問題に関する新しい声を取り入れることに努力する。

②国際組織と複数利害関係者組織（Multi - stakeholder Organization）：地域組織は、特に彼らのメンバーに特有のサイバーセキュリティ問題に対処するのに効果的であった。地域組織は、行動規範を開発・適用する分野でますます重要な役割を果たしている。我々は、メンバーの具体的な利益を実現することのできる各組織の専門知識・技術に適した生産的な課題を明らかにするために、より広範な国際組織のみならずこれらの地域組織にも参加し続ける。インターネット・ガバナンス政策については、対応性と国際的な代表制度を確実にするための重要な措置が取られた。米国は、それらの努力に敬意を表する。そして、米国は、複数利害関係者の環境において、政府のみならず、民間セクター、市民社会、学界が統合されたインターネット・コミュニティ全体を代表するようなフォーラムの独特な貢献を認めている。

③民間セクターとの協働：民間セクターは、すでに国際組織及び複数利害関係者組織において重要な役割を果たしているが、我々は、産業界の仲間を引き込むために、既存のパートナーシップ機構を活用し続ける。特に、我々は、ネットワークのエコシステムを保全するイニシアティブを拡大し、サイバー空間の利益と特質を維持し、技術的進化にとって不必要な障害を回避し、そして、平和と安全保障の原則を拡大するために、インフラの所有者及びネットワークの機能性の大部分について責任を有している運営者双方と緊密に連携する。また、我々は、複数利害関係者の特徴を守るために不可欠であるインターネット・ガバナンスへの民間セクターの参加を求めるとともに、そのような問題に取り組むフォーラムへの民間セクターの参加を提唱し続ける。

(2) 防衛：拒否的抑止（dissuading）と制裁的抑止（deterring）

脅威がテロリスト及びサイバー犯罪人からのものであっても、あるいは国家及びその代理人からのものであっても、米国はそのネットワークを防護する。同様に重要なことは、我々は良心的なアクターを奨励し、サイバー空間の平和と安定を脅かすアクターを抑止することである。我々は、国家及び国際ネットワークの弾力性、監視能力、及び多数の信頼できる対応措置を統合した重複した政策で拒否的抑止（攻撃者の特定の目的達成を拒否する能力を持つことにより、目的達成が不可能であることを認識させ、攻撃の意図を起こさせない。(訳者注)）及び制裁的抑止（報復力により、耐えられない制裁を加えるという脅しによって、攻撃を自制させる。(訳者注)）を行う。すべての我々の防御努力において、我々は我々の法律と原則に基づき、人権とプライバシーを保護する。

防衛目標
米国は、他の国々と共に、責任ある行動を奨励し、ネットワークとシステムを混乱させようとする人々に反対する。そして、悪意のあるアクターを抑止し、死活的に重要な国家資産を必要に応じ適切に守る権利を留保する。

ア．拒否的抑止（Dissuasion）

大きな価値のあるネットワークを保護するためには、強固な防御能力を必要とする。米国は、ネットワークの防御能力と、混乱やその他の攻撃から持ちこたえ、回復する我々の能力を強化し続ける。損傷をもたらす、より洗練された攻撃に際し、我々は、我々のネットワークへの影響及び他のネットワークへの波及を限定し、システムの混乱を局限かつ軽減するために、良く練られた対応計画に基づき行動する。

(ア) 国内の強化

我々のネットワークと情報システムの弾力性を確保するには、政府全体に及ぶ統一した国

家行動を必要とする。民間セクターや個々の市民との連携も必要である。この 10 年間、米国は、サイバーセキュリティの文化を育成し、リスク軽減とインシデント対応のための効果的な装置を開発してきた。我々は、公共セクターと民間セクターにおけるベストプラクティスの組織的な適用は国家の脆弱性を減少させ、そして、ネットワークとシステムを強化することを強調してきた。また、我々は、公共セクターと民間セクターのネットワークの脆弱性とリスクに関する状況認識(situational awareness)の共有に関して着実に前進している。我々は、国家コンピュータ・セキュリティ・インシデント対応チームを通じて、政府、主要な産業、我々の重要なインフラセクター、及びその他の利害関係者の間の情報共有のための新しいイニシアティブを構築した。また、我々は、民間セクターと政府の両者が依存するシステムンのセキュリティを強化するために、民間セクターとのパートナーシップを強化する方法を求め続けている。

(イ) 国外の強化

防衛のこのモデルは、教育、訓練、及び現行の作戦、並びに政策上の協力関係を通じて、成功裏に国際的に共有されている。今目、技術及び軍事分野における既存及び発展中の協力関係を通じて、インシデントに対応する先例のない能力を共有している。これは、我々の国家及び国際ネットワークに長期的な損傷を与えようとする敵対者の能力を拒否するための重要な処置である。しかし、地球規模に分散されたネットワークは、地球規模の分配配置された早期警戒能力を必要とする。我々は、地球規模で新しいコンピュータ・セキュリティ・インシデント対応能力を創造し続けなければならない。そして、それらの相互接続を容易にするとともにコンピュータ・ネットワーク防御を強化し続けなければならない。米国は、発展途上国が防衛能力を構築するのを支援することに共通の利益を有している。そして、我々のパートナーと協カして、この領域に我々の力を注入する。友好国や同盟国との協力関係の構築は、国際社会全体の集団安全保障を強化する。

イ．制裁的抑止（Deterrence）

米国は、我々のネットワークに対する攻撃又は情報収集に伴うリスクが（攻撃者の得ようとする）潜在的な利益を大きく上回ることを確実とする。我々は、サイバー空間上の行動がネットワークを越えて大きな影響を与えることを十分に認識している。そのような事象は、自衛のための対応を必要とするかもしれない。同様に、相互接続したネットワークは、より密接に国家同士を結び付けている。故に、ある国のネットワークへの攻撃は、国境を遠く離れた国に影響を与えるかもしれない。我々の国家及び経済安全保障を脅かす犯罪者及びその他の非国家主体の場合、国内的には、彼らを抑止するためには、国内外のネットワークに侵入又は混乱させた犯罪者を捜査し、逮捕し、そして起訴するプロセスをすべての国が整備していなければならない。国際的には、各国の法執行機関は、お互いと協力しなければならない。また、法執行機関は、できる限り、進行中の捜査に不可欠な劣化しや

すいデータ(perishable data)を常に更新し、捜査方針を調整するために議会及び司法省と協力し、そして、正当な法手続きと法の支配を促進しなければならない。これらはすべてサイバー犯罪条約(Budapest Convention on Cybercrime)の主要な信条である。そうすることが正当な場合、米国は、サイバー空間における敵対的行為に対応する。それは、我が国への他のどんな脅威に対しても対応することと同じである。すべての国は、固有の自衛権を保有している。そして、サイバー空間で実行される特定の敵対的行為は、我々の軍事条約パートナーとの公約の下での行動を余儀なくさせるであろうことを我々は認識している。我々は、我々の国家、同盟国、パートナー、及び利益を守るために、必要に応じてかつ適用される国際法に基づき、すべての必要な手段（外交、情報、軍事、及び経済)を使用する権利を留保する。そうする際に、我々は、可能な限り、軍事力を使用する前にすべてのオプションを使い果たすであろう。我々は、注意深く、行動した場合のコストとリスクを、行動しない場合のコストと比較検討する。そして我々は、可能な限り幅広い国際的支持を求めながら、我々の価値を反映するとともに合法性を強化する方法で行動する。

(3) 開発：繁栄とセキュリティの構築

米国は、接続された世界の恩恵は普遍的であるという我々の信念を示し続ける。サイバー空間の開放性、相互運用性、セキュリティ、及び信頼性の価値は、今目以上に利用できなければならない。そして、世界の情報・経済のリーダーとして、米国は、我々の技術的な資源と専門知識が人々に利益をもたらすことを確実にすることを確約する。
米国は、新規及び既存のデジタルシステムを構築し、サイバーセキュリティに関する知識と能力を提供する積極的な役割を果たす。そうしながら、各国が責任ある利害関係者として行動するというコンセンサスを構築する。これらの目標を実現するためには、短期的な支出でなく、賢明な長期的な投資と関与を継続するという政府の公約が必要である。

開発目標
米国は、二国間や多国間の組織を通して、国外のサイバーセキュリティ能力の構築を促進する。そうすることにより、各国は、公開性、相互運用性、セキュリティ、及び信頼性のあるネットワークに関するコンセンサスの下、デジタル基盤を保護し、地球規模のネットワークを強化し、そして、密接なパートナーシップを構築することができる。

ア．技術的能力の構築

ネットワーク化技術へのアクセスはますます発展のための基本的欲求となっている。政府と産業界は、サービスが提供されていない又は提供されている地域全体の接続性を向上するために、いくつかの意義のある措置を講じた。国際的な情報インフラは成熟し、拡大し続けている。そして、より多くの国々に対して地球規模の情報の流れにアクセスする機会

を提供している。世界規模のネットワークの成長とそれへのアクセスの拡大は、国際社会を豊かにするが、その一方で伝統的な間題とサイバーセキュリティの協働に関する新しい挑戦と好機を提示している。これらの能力の多くは民間セクターの投資の結果である。そして、米国は、各国の政府や産業界と協力して友好的な雰囲気を構築し、各国が重要な開発ニーズに取り組み易い環境をつくる。
政府は、この新しい接続性が有益な結果を生むかあるいはその可能性を無駄にするかどうかの主要な決定要因である。我々の能力構築取組（capability - building efforts）から利益を得た国々は、政治的な支配のためにアクセスを制限するよりはむしろ、繁栄と社会的結合を強化するために技術を受け入れる国々である。従って、米国が支援する技術プロジェクトは、意図的に、セキュリティと商業を強化し、情報の自由な流れを保護し、そしてネットワークの地球規模の相互運用性を促進する。

イ．サイバーセキュリティ能力の構築

繁栄は、恐れや信頼性の欠如の上には築くことができない。米国は、各国が自身の技術開発とともにサイバーセキュリティ能力を構築するのを手助けすることを確約する。発展途上国の国家レベルのサイバーセキュリティを強化することは緊急かつ長期的な利益である。そして、多くの国々は、彼らの国境内に次々と現れる脅威に立ち向かい、地球規模で相互接続したネットワークの信頼性を築いている。そして情報技術の犯罪的な不正使用を防止するために国境を越えて協力する態勢が整ってきている。また、サイバーセキュリティの次世代の挑戦に対応できるダイナミックな国際的研究コミュニティを育成することが必須である。

サイバーセキュリティがすべての国の責任として国家的努力によって対処されなければならない地球規模の間題であることを認識し、我々は、サイバーセキュリティ能力構築(意識向上、法的訓練、及び技術的訓練の強化並びに政策策定の支援)に焦点を合わせたイニシアティブを拡大・正規化する。そのようなプログラムは、単に技術以上のものとして取り組まなければならない。我々は、サイバーセキュリティ挑戦の幅を知るために各国と連携し、彼ら自身の戦略策定を援助し、そしてネットワークセキュリティ及びコンピュータ緊急事態対応チーム(Computer Emergency Readiness Team：CERT)の設立から、国際的な法執行及び防衛協力、並びに国内及び国外の民間セクター及び市民社会の生産的な関係までのすべての分野の能力を構築する。

ウ．各国の政策との関係性の構築

米国の能力構築援助（capability - building assistance）は、投資、深い関与、並びに対話及び協力の重要な機会として構想されている。各国がサイバー空間に関する間題への取り組みを深めるのに伴い、我々は、能力構築から、ともに懸念を有する間題について、経済、

技術、法執行、防衛、及び外交面での活発な協働にまで、我々の対話を成熟させるつもりである。また、我々は、専門知識及び技能を有する地域フォーラム及び技術的組織の両方を使って自国のサイバーセキュリティ能力を開発している国々との間の結びつきを促進する。そして、我々は、ベストプラクティス、教訓、及び国際的な技術交流を促進し続ける。

第 3 章　政策の優先事項

米国は、米国民と国際社会の人々双方のために、国内外で開放性、相互運用性、セキュリティ、及び信頼性のあるネットワークを構築・維持するのを支援するための行動を継続する。我々のアプローチは、基本的な原則によって導かれ、包括的な目標によって推進され、そして米国の国際サイバー空間戦略の基礎を形づくる本戦略で示された方針によって遂行される。

サイバー空間がすべての人々のためにその可能性を十分に発揮するという将来を実現するために、米国政府は、7 つの相互依存した領域における活動を組織化する。それぞれの活動では、我々の政府機関、国際パートナー、及び民間セクターとの協働が強く求められる。

全体として見れば、以下の 7 つの領域での活動は、我々の戦略的フレームワークの要処置限界値(action line)を形成する。米国政府の多くの省庁は、すでにこれらの活動に携わっている。以下の 7 つの領域での活動は、すでに進行中の重要な作業を補強するものである。サイバー空間における特定の責任を遂行する実施計画を作成している人々に対して、本章は、背景を説明し、努力の統一を確実なものとする。また、ここで概説される「政策の優先事項」は、国家レベルの努力の統一と資源を必要とする過去、現在、及び将来の領域を明確にするとともに、要求される特定の行動とその指針を示している。

１．経済：国際標準、イノベーション、及び「開かれた市場」の促進

サイバー空間が我々の経済とイノベーションの要求に応え続けることを確実にするために、我々は以下のことを行う。

①アクセスし易く、地球規模で接続されたネットワークに関する技術的イノベーションを促進する自由貿易環境を維持する。: 情報の自由な流れが我々のネットワークの機能にとってきわめて重大であるように、自由貿易は、情報化時代のイノベーションと市場拡大を促進する。インターネットが世界中で受け入れられたのは、主として低価格で世界中で使用できるコピュータとネットワーク技術が広まったことに由来する。自由貿易環境は、メーカーに価格を低く抑えかつ品質を高めることを要求するので、これらの市場における競争はイノベーションを推進する。技術開発と貿易の国際標準を尊重することは、開かれた市場を支える根幹であり、さらに最先端技術を持った企業は、彼らの革新的な製品とサービスの恩恵を広く提供することが可能となる。次の 2～30 年の間、製造技術の国際化は進み、我々のネットワークと消費者に相当の恩恵をもたらすであろう。米国は、その自由貿易環境を維持するために努力する。そして、将来のイノベーションを確実にするために、特に

ハイテクセクター（先端技術部門）を支援する。

②企業秘密を含む知的所有権を窃盗から保護する。: 地球規模のネットワークは、イノベーションの原動力ともなるが、一方で産業スパイ並びに知的所有権及び営業情報の窃盗のリスクを高めている。サイバー空間を使用して、先例のない情報量を企業、大学、及び政府機関から盗むことができる。そのようにして盗まれた情報と技術の損失額は、何十億ドルにもなる。個別のサイバー空間インシデントには、しばしば報告されてないかあるいは探知されていないものがある。インシデントの結果は、不正競争から企業全体の倒産にまで及ぶ。中にはその国家的影響が、桁の違う大きな規模になる場合がある。知的所有権の永続的な窃盗は、犯罪者、外国企業、又は国家アクターであろうとなかろうと、（企業の）世界経済の競争力を弱め、イノベーションの機会を奪うことができる。そのような行為が違法であり許されないことを認め、そのようなアクターに責任を取らせるという国際環境を構築するために、米国は、そのような行為を特定し、対応するための方策を講じる。

③技術者が決定した相互運用性とセキュリティに関する技術基準の優位性を確実にする。: 国際的、自発的、そしてコンセンサス・ベースによりサイバーセキュリティの国際基準を開発すること、並びにそのような基準に基づく製品、プロセス、及びサービスを展開・販売することは、相互運用性、セキュリティ、及び弾力性を有した地球規模のインフラの基礎である。公共及び民間セクターは、これらの基準を開発・維持・実装して、国際通商貿易の障壁ができるのを防ぐための国際標準と適合性審査スキーム（conformity assessment schemes）の開発を支援するために協力しなければならない。サイバーセキュリティ国際標準化、そして、その自発的かつコンセンサス・ベースのプロセスは、全体の利益にかなっている。サイバーセキュリティの標準化は、イノベーションを促進し、相互運用性、セキュリティ、及び弾力性を強化し、そしてオンライン取引における競争を促進する。米国は、製品とサービスのための国際標準ベースの要件(requirements)の普及を確実にするために、公共及び民間セクター間の協働を促進する。

２．我々のネットワークの防護：セキュリティ、信頼性、及び弾力性の強化

強固なサイバーセキュリティは国家及び経済安全保障にとって極めて重要である。ゆえに、我々は、以下のことを行う。

①二国及び多国間の組織、並びに多国間のパートナーシップを通じて、サイバー空間に関する協働、とりわけ国家の行動及びサイバーセキュリティの規範についての協働を促進する。: ますます多くの国際組織がサイバーセキュリティとその他のサイバー空間の問題に取り組んでいる。米国は、この重要な作業を促進する。そして、多様な参加者の要求に応じ

て、様々な作業の中にサイバー問題を組み入れる。我々は、関連するサイバー空間問題を、米州機構(Organization of American States：OAS)、東南アジア諸国連合(Association of Southeast Asian Nations：ASEAN)、アセアン地域フオーラム(ASEAN Regional Forum：ARF)、欧州安全保障機構(Organization for Security and Co-operation in Europe：OSCE)、G-8、欧州連合(European Union：EU)、国連(United Nation：U.N.)、及び欧州評議会(Council of Europe)の議題に組み入れるために努力した。また、我々は、作業が効果的な制度的枠組みによって支援されることを確実にするために努力した。米国は、これらのフォーラム及びその他のフォーラムで、規範を含み鍵となるサイバー空間活動についての地域的及び国際的コンセンサスを取り纏めている。我々は、本戦略で概説されているインターネット政策の原則を精緻化するために、複数利害関係者の協働とコンセンサス構築を可能にするフォーラムにも関心を持っている。我々は、世界規模の能力の構築への我々の関心を推進するために、この作業を、現在対話への代表が少ない地域、特に、アフリカと中東へ拡大することを歓迎する。

②米国のネットワークへの侵入とそれの混乱を減少する。：無許可のネットワーク侵入は、経済の健全性を脅かし、国家安全保障を侵食する。米国政府の各機関は、産業スパイからイノベーション技術を保護し、連邦政府及び地方政府のネットワークワークを保護し、軍事作戦を劣悪な作戦環境から保護し、侵入及び攻撃から最重要インフラ、特に、エネルギーシステム、輸送システム、金融システム、又は防衛産業基盤を保全するために、民間部門と協力する。米国は、所有権の尊重とネットワークの安定性の重要性を認めることについて幅広い国際的コンセンサスの確立を追求する。そして、我々及び我々のパートナーは、ネットワークを危殆にさらす行為から我々のネットワークを防護するという信念を堅持する。

③情報インフラのための強固なインシデント管理能力、弾力性（resiliency)、及び回復能力（recovery capabilities）を確保する。：地球規模で相互接続された環境では、ある国のシステムのセキュリティの脆弱性は、他の国のシステムに対するリスクを増大させる。どの国も、地球規模のネットワークに関する完全な洞察を持つことはできない。事象が、我々すべてを脅かすかもしれない時、我々には、他の国々と、我々自身のネットワークについての我々の洞察を共有し、協力する義務がある。我々は、我々自身の対応能力を構築・強化しながら、より大きな地球規模の状況認識とインシデント対応能力を有する国際ネットワークを拡大するために他の国々と協力する。米国政府は、海外パートナーの信頼できるネットワークとの情報交換を通じて、監視、警報、及びインシデント対応に積極的に参加する。また、我々は、総合的な弾力性を強化するために国際的な協働を通じてこれらの能力を拡大する。さらに、米国は、我々のパートナーと共に確立した運用手順を改善・強化するためにサイバーセキュリティ演習への参加を各国に呼び掛ける。

④企業との協議を通じて、ハイテク・サプライチェーンのセキュリティを改善する。: 最重要なネットワークと情報インフラの運営は、信頼できるハードウェアとソフトウェアの確実な可用性に依存している。サプライチェーンの脆弱さは、ネットワークとその中のデータの完全性、可用性、及び機密性への攻撃を可能にすることができる。これらの脆弱性の利用は、経済活動と国家安全保障を弱体化させる。米国は、情報システムと最重要なインフラの完全性を保護するためのベストプラクティスを開発するために、産業界及び世界のパートナーと協力する。このようにして、我々は、自由で開放的な貿易が依存しているグローバルなサプライチェーンのセキュリティを強化する。

３．法執行：協働と「法の支配」の拡大

サイバー空間の信頼性を強化し、オンライン・システムを悪用する人々を捜索するために、我々は以下のことを行う。

①国際的なサイバー犯罪政策の開発に完全に参加する。: 米国は、実績のある専門知識と効果的なサイバー犯罪政策を推進した歴史を有するフォーラムにおいてサイバー犯罪の国際的な規範と対策を開発する方法に関する二国間及び多国間の議論に積極的に参加することを公約している。これらの議論には、ブダペスト条約のような制度を如何に拡大するかなどの既存の努力も含まれる。米国は、国内の法執行機関との良好なパートナーシップと我々が現在享受している生産的な政策対話の上にこれらの取り組みを構築する。そして、この取り組みに参加している国々の責任感を育成する。

②ブタペス条約の加盟国を拡大することによって、サイバー犯罪を取り締まる法律を国際的に一致させる。: サイバー犯罪事件を捜査・起訴する際に、米国も我々の同盟国も、他の国々の協力と支援に頼らざるを得ない。各国が共通のサイバー犯罪関連法律を整備しているとき、この協力は最も効果的かつ意義がある。そこでは、証拠の共有、身柄の引き渡し、及びその他の協力が容易となる。サイバー犯罪に関するブタペスト条約は、各国に法律の起草と現行法の改正のためのモデルを提供している。そして、それはサイバー犯罪事件に関する国際協力を強化するための効果的な仕組みであることが証明されている。米国は、他の国々が条約の締約国になることを促進し続けるとともに、現在の非締約国が彼ら自身の法律の基礎としてこの条約を使用するのを手助けする。こうすることにより、短期的には二国間の協力を容易にし、長期的には彼らがこの条約に加盟する可能性が大きくなる。

③インターネットへのアクセスを制限するのでなく、違法な活動を取り締るサイバー犯罪関連法律を重視する。: サイバー空間における犯罪行為は、合法的なアクセス又はインター

ネット上のコンテンツを制限するのではなく、効果的な法執行により対処されなければならない。この目標を達成するために、米国政府は、アクセスの幅広い規制は、無実のインターネット利用者に影響を及ぼすので、インターネットへのアクセスを広範に制限するよりはむしろ、犯罪を防止し、そして犯罪者を逮捕・処罰することを重視することによりオンライン犯罪に対処すべきであることを、二国間及び多国間協議を通じて各国に呼びかけている。米国と我々のパートナーは、世界中の法執行組織の能力構築を支援する際に、プライバシー、基本的自由、及びイノベーションの保護というアプローチとサイバー空間の犯罪防止というアプローチを一体化して取り組んでいる。

④テロリストやその他の犯罪者が、作戦計画立案、資金調達、又は攻撃のためにインターネットを利用する能力を拒否する。: 米国はサイバー犯罪に関する様々な国際的な能力構築や訓練プログラムを保有している。そして、法執行機関と議会が、テロリストとインターネットを不正使用する犯罪者を捜査・起訴するための、効果的な法的枠組みと専門知識を開発するのを手助けしている。テロリストが、「雇われハッカー」や組織犯罪ツールを利用して能力を強化することを防止することは、国際社会にとって重要な優先事項であり、そのために、効果的なサイバー犯罪関連法の整備が強く要求される。米国は、金融活動作業部会(Financia1 Action Task Force)のような技術的ツールと国際協力フレームワークを通じて、テロリストとサイバー犯罪金融ネットワークを調査し、崩壊させることを公約している。

４．軍事：２１世紀の安全保障上の課題への備え

我々の市民、同盟国、及び利益を防衛するという公約は、どこで脅かされようとも拡大適用される。したがって、我々は、以下のことを行う。

①信頼できかつセキュアなネットワークに対する軍隊のニーズの増加を認識し、それに適応する。: 我々は、我々の軍隊がますます、彼らを支援するネットワークに依存していることを認識している。そして、我々は、敵対者がそのシステム又は国防に不可欠なインフラを混乱させようとする環境においても、我々の軍隊が十分に軍事行動を遂行する能力を備えたままでいることを確実とするために努力する。米国は、あらゆる国と同じように、我々の重要な原則及び価値と同様に重要な資産を防衛することに非常に強い関心を有している。そして、我々はそうする我々の能力を妨げようとする者からそれらを防衛することを公約している。

②サイバー空間における潜在的な脅威に立ち向かうために、既存の軍事同盟を強化する。: どんな国も単独では、サイバーセキュリティを達成することはできない。我々のネットワ

ークを混乱させるか、又はそこから情報を窃盗しようとする敵対者に立ち向かうためには、より大きなレベルの国際協力が必要である。この努力は、NATO のような我々の最も親密な同盟国と相互接続し、ネットワーク化されたシステムが新しいリスクに晒されていることを認識することから始まる。そこから前進し、米国は、状況認識と警報システムの共有を拡大し、平和と危機のときに協力する我々の能力を強化する。特に、サイバー空間における集団防衛の手段と方法を開発するために、我々の同盟国及びパートナー国の軍民のカウンターパートとの協力を促進する。かかる軍事同盟とパートナーシップは、我々の集団的抑止能力を支え、国家主体及び非国家主体の敵対者から米国を防衛する能力を強化する。

③集団安全保障を増進するために、同盟国やパートナー国とのサイバー空間での協働を拡大する。: また、サイバー空間の挑戦は、同盟国及びパートナー国の軍隊に、新しい方法で協力する機会をもたらしている。標準運用手順（standard operating procedures：SOP）の理解を共有することによって、我々の軍隊は、調整とより大きな情報交換を通じてセキュリティを強化することができる。これらにより、（敵対国の）軍の活動に関する誤解を小さくし、対立がエスカレーションする可能性を小さくすることができる。電子情報の科学捜査(デジタルフォレンジック)や人員の育成などの対話とベストプラクティスの共有はパートナーの能力を強化する。また、（同盟国やパートナー国との）ネットワーク侵入テストや弾力性テストは、この努力にとって重要である。米国は、同じ考えを持った国々と緊密に連携しながら、サイバー空間における悪意ある行為を阻止するために、対処能力を向上し、全体的なリスクを削減し、複数利害関係者のイニシアティブを促進する。

５．インターネット・ガバナンス：効果的で誰にでも受け入れやすい構造の促進

効果的にすべてのインターネット利用者のニーズを満たすインターネット・ガバナンス構造を促進するために、以下のことを行う。

①インターネットの開放性とイノベーションを優先させる。: 効率的にインターネット上に情報を配信する能力は、現代の消費者、ビジネス、政治、科学、及び教育活動のまさしく中核である。世界のあらゆる政府は、インターネットの価値を認めている。しかし、彼らの多くは、恣意的に、情報の自由な流れを制限したり又は反対意見や反対活動を抑制している。これらの規制の方法と実行は国ごとに大きく異なるかもしれない。しかし、我々は、基本的自由を侵し、又は不必要にイノベーションを抑制するために、彼らが正当性を主張するようなインターネット・ガバナンス又は技術的アーキテクチャーを再設計することを許してはならない。効果的かつ広範囲の考えを取り入れたインターネット・ガバナンスは、許容できるネットワーク管理の国際規範から著しく外れた行為が、技術的又は統治構造によって一層悪化することを防止することに役立つ。開放性のある地球規模のインターネッ

トへのアクセスを維持・強化・増加することが明白な政策の優先事項である。米国は、適切な複数利害関係者の組織、関連する国際組織、及び NGO への支援を通じて、これらの目標を前進させる。

②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セキュリティと安定性を維持する。: 世界経済に対するインターネットの重要性を考えれば、複数のネットワークで構成されるこのネットワークとそれを支えている基盤(DNS)が安定かつセキュアであり続けることが重要である。この継続した安定性とセキュリティを確実にするために、我々と同様に他の世界の国々が、インターネットの技術的な運用に不可欠な利害関係者の貢献、特にその組織と技術者の貢献を認識することが必須である。米国は、これらの資源の効果的な調整がインターネットの成功を促進することを認識し、効果的な複数利害関係者プロセスを支援し続ける。

③インターネット・ガバナンスの課題に関する複数利害関係者の討議を促進・強化する。: インターネットのまさしくそのアーキテクチャーは、分散化、共同化、及び階層化された社会的及び技術的な組織モデルを具体化している。これらの特徴は、インターネットがもたらす恩恵の基礎となる。そのアークテキチャーは、社会的及び政治的な成長を可能とする表現と結社の自由を刺激し、さらには民主主義社会の発展を刺激する。米国は、国際社会が様々なインターネット・ガバナンスに関する問題を討議する際には、複数利害関係者方式で実施すべきであるという固い信念を持っている。我々はインターネット・ガバナンス・フォーラム（Internet Governance Forum：IGF）のような成功した会議を支持する。そのフォーラムは、非政府の利害関係者が、政府と対等の立場で討議に貢献することができるなど、開放的で誰でも受け入れるというインターネットの性質を具現化している。

６．国際的な開発：能力（Capacity)、セキュリティ、及び繁栄の構築

地球規模にネットワーク化された技術の恩恵を促進し、我々の共有ネットワークの信頼性を強化し、そして、サイバー空間に責任を有する利害関係者のコミュニティを構築するために、我々は以下のことを行う。

①技術的能力及びサイバーセキュリティ能力を構築しようとしている国に対して、必要な知識、訓練、及びその他の資源を提供する。: 相互接続された世界の恩恵は、国境によって制限されてはならない。10 年以上の間、米国は、他の国々が技術とサイバーセキュリティに関する主要な能力を構築するために必要な資源と技能を取得するためのさまざまなプログラムを支援してきた。我々の目標は、他の国々が我々の経験から学ぶことを手助けすることである。特に、サイバーセキュリティを彼らの国家的な技術開発計画に組み入れるこ

と援助する。ニーズは多くかつ多様であるので、我々のプログラムはインシデント管理の国家能力の強化から、公共と民間パートナーシップの構築、制御システムのセキュリティの強化、サイバー犯罪を捜査・起訴するための法律の立案、並びにサイバーセキュリティ認識向上及びサイバーセキュリティの国家的文化の構築のためのプログラムの策定・履行にまで及ぶ。我々の支援は、米電気通信研修所(United States Telecommunications Training Institute : USTTI)のような革新的な官民イニシアティブに基づくパートナーシップと同様に、二国間の対外援助として行われた。近年、我々は多国間のフォーラム、例えば米州機構(Organization of American States : OAS)、アジア太平洋経済協力(Asia-Pacific Economic Cooperation : APEC)及び国連（United Nations : U.N.)において、この支援を最優先事項にするのに大きな役割を果たした。米国は、これらの官民の協力を拡大し、能力向上への民間部門の投資を促進するために国内で活動し、この最重要なニーズへの関心を高め、これから数年のうちに、新しい協働の枠組みを構築するために努力する。

②国際的なサイバーセキュリティに関するベストプラクティスを絶えず開発し、それを共有する。: 今日、国家はもはや試行錯誤のプロセスを通じて、排他的にサイバーセキュリティ能力を高める必要はない。我々は、各国がより賢い投資をして、より効果的な政策を立案するのを手助けすることを目的としたベストプラクティスを開発・共有するために、数十の国々及び多数の多国籍組織と協力する。米国は、ベストプラクティス、協働における技術的基準、及び企業との緊密なパートナーシップを特定・開発・改善し続ける。そして、それらの認知度と利用を促進するための我々の努力を拡大する。我々は、サイバーセキュリティ・ツールと能力を強化するための共同の科学技術研究をさらに促進する。

③サイバー犯罪と闘う国家の能力を強化する。それには、法執行機関、科学捜査専門家、法律専門家、及び国会議員に対する訓練が含まれる。: コンピュータ・ネットワークに関連した犯罪事案ではしばしば海外に存在する証拠と標的(Target)が関係するので、各国政府は、広範な技術的及び捜査上の支援にお互いに依存している。インターネットで接続された国のいずれもが、犯罪脅威の起源となる。そして、多くの国は、そのような捜査に必要な捜査能力を開発するための相当な援助を必要としている。これらの訓練を提供することによって、我々は、重要な二国間関係を発展させるとともに、当該国が法執行に関する技術的な理解を深めるのを支援する。この関与は、効果的な法執行協力と相互支援の可能性を大きくする。米国は、アジア太平洋経済協力（APEC）、東南アジア諸国連合（ASEAN）、G-8、及び米州機構（OSA）と協力しながら、それらの地域の国々へ、あるいはアフリカの国々への我々の関与を継続しながら、多くの国々において、この目標を追求する。

④専門家や米国政府のカウンターパートとの定期的かつ継続した接触を提供しながら、技術的能力構築のために政策立案者との関係を発展させる。: 過去 2、3 年の間に増大しつつ

あるサイバー空間間題に取り組む政策担当者間の国際的コミュニティは、新しい対話の場を提供し、新しい開発とセキュリティに関するイニシアティブを立ち上げるとともに無数の二国間関係を強化した。技術的及びサイバーセキュリティ能力の構築を通して、発展途上国の遠い将来に投資しながら、米国はこれらの援助関係を、共通の懸念を有する問題についても話し合える、より緊密なパートナーシップに発展させるよう努力する。我々は、例えば最重要な情報インフラの防護間題に関する協働を促進するメリデイアン国際会同(Meridian Conference)のようなフォーラムで先導的な役割を果たした。米国は、サイバー空間の将来への投資が増大されるに伴い、より多くの国が対話に参加することを歓迎する。そして、米国は、我々の専門家及び政策担当者とそれらの国のカウンターパートとの間の永続的な関係の構築に努力する。

７．インターネット自由（Internet Freedom）：基本的自由とプライバシーの支持

サイバー空間におけるプライバシーだけでなく、基本的自由を保護するために、我々は以下のことを行う。

①市民社会のユーザーが、表現と結社の自由のために、信頼でき、セキュアで、かつ安全なプラットフォームを使うことを支持する。: 我々は、世界中の人々が意見を表明し、情報を共有し、選挙を監視し、腐敗を暴露し、並びに社会的及び政治的運動を組織するためにデジタルメディアを使用することを奨励するとともに、これらの技術を使用する人々に対して嫌がらせをし、不正に逮捕し、脅し、又は暴力を振るう人々を非難する。そのような恐怖の文化は、コミュニティの人々が、考えを伝え、体系化し、交換するために新技術を使用しようとする意欲を失わせる。同様の保護が、インターネット・サービス・プロバイダ及びその他の接続プロバイダにも適用されなければならない。それらの業者は、しばしば合法的なスピーチを検閲する法的義務を仲介業者に課している法体制の犠牲になる。米国は、サイバー空間を通しての表現と結社の基本的自由を根気強く提唱する。我々は、デジタルメディアを使用する市民社会のユーザー、人権擁護団体、及びジャーナリストに力を与えるために努力する。また、我々は、各国の政府に対し、表現の自由や情報の自由な流れを不適切に制限する責任を企業に課すより、むしろ政府が真のサイバー空間の脅威に取り組むことを強く奨励する。

②市民のインターネット活動を違法なデジタル侵入から保護するための防護措置を確立するために市民社会及び NGO と協働する。: 市民社会と NGO のサイバーセキュリティを促進することは、デジタル時代の表現と結社の自由がより広く享受されることを確実とする手助けとなる。サイバーセキュリティは、最前線の活動家、擁護団体、及びジャーナリストにとって特に重要である。彼らは、世間一般の人々の気に入らない考えや意見を表明す

るかもしれない。そして、彼らは、しばしば彼らの電子メール・アカウント、ウェブサイト、携帯電話、及びデータ・システムへの侵入・混乱の犠牲者となる。米国は、これらのユーザーに、彼ら自身を防護するための力を与える努力を支援し、彼らの自由な表現と結社の権利を行使する彼らの能力を 21 世紀の新技術によって保護するのを手助けする。

第 4 章　将来に向かっての前進

ネットワーク化技術の恩恵は、特権を有する数か国又はそれらの国の少数の人々のためだけのものではない。しかし、接続性はそれ自体が目的ではない。それは、イノベーションに対して門戸が開かれ、世界中で相互運用性があり、人々の信頼を得るに十分なセキュリティがあり、そして彼ら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いう目的のための手段である。

30 年前、ほとんどの人は、インターネットと呼ばれるものが、我々の仕事と生活に革命を起こすことを理解できなかった。この短い期間に、数百万の人々は、現在、彼らの生活様式、さらに生活さえもネットワーク化技術の恩恵を受けるようになった。10 億人以上が、日常的な社会的交流においてそれに依存している。この技術は、前の世代の人々がほとんど不可能であると考えていたことを可能にしながら、社会を前進させている。米国は、米国と世界中の人々の創造力と想像力を刺激し続ける。我々は、次の大きなイノベーションが何であるかを知ることはできないが、それが形となり繁栄する世界を実現することに全力で取り組む。

本戦略は、米国政府の各省庁が国際サイバー空間政策における彼らの役割を定義・調整すること、具体的な方法を実行すること、そして、将来の実施計画を立案することを可能とするためのロードマップである。本戦略は、パートナーシップ、認識、及び行動を通じて、これらの努力を補強するために民間セクター、市民社会、及びエンドユーザーへ呼びかけるものである。最も重要なことは、本戦略は、我々のネットワーク化された世界の繁栄、セキュリティ、及び開放性という展望を実現するために、他の国々及び人々に対して我々に加わるよう勧誘するものである。これらのアイデアが、我々が理解しているサイバー空間を維持し、我々が求める将来を共に築くために最も重要なことである。

平成２１・２２・２３年度発刊資料

ＢＳＫ 第２２－ １号『標 的 に さ れ る 合 衆 国 技 術』
ＢＳＫ 第２２－ ２号『我が国をめぐる兵器技術情報管理の諸問題（平成 21 年度）』
ＢＳＫ 第２２－ ３号『カウンターインテリジェンスの最前線に位置する防衛関連企業の対策について（平成 21 年度）』
ＢＳＫ 第２２－ ４号『新しい防衛調達モデルの探索的調査研究（その３）』
ＢＳＫ 第２２－ ５号『中華人民共和国のサイバー戦とコンピュータ・ネットワーク・エクスプロイテーション能力』
『米中経済安全保障調査委員会議会報告 2009 から抜粋』
ＢＳＫ 第２３－ １号『セ キ ュ リ テ ィ 計 画 立 案 の ガ イ ド』
ＢＳＫ 第２３－ ２号『サ イ バ ー ス ペ ー ス 政 策 の 再 検 討』
ＢＳＫ 第２３－ ３号『我が国をめぐる諸外国の技術情報等の取得活動と波及問題』
ＢＳＫ 第２３－ ４号『グローバル IT 社会におけるサイバーセキュリティの脅威に対するリスクマネジメントについて（平成２２年度）』
ＢＳＫ 第２３－ ５号『わが国の防衛調達改革におけるＣＰＴ実現のための調査研究』
ＢＳＫ 第２４－ １号『サ イ バ ー 空 間 の た め の 国 際 戦 略』

本報告書の中で意見にわたるものは、委託研究先の見解であることをお断りしておきます。

サ イ バ ー 空 間 の た め の 国 際 戦 略

(INTERNATIONAL STRATEGY FOR CYBERSECURITY)

平成２３年１０月　発行
非 売 品　　禁 無 断 転 載・複 製
発　　行　：　財団法人　防衛調達基盤整備協会
編　　集　：　防衛調達研究センター刊行物等編集委員会
〒160-0003　東京都新宿区本塩町２１番３－２
電　話　：　０３－３３５８－８７５４
ＦＡＸ　：　０３－３３５８－８７３５
メール　：　hozen@bsk-z.or.jp
ＢＳＫホームページ：　http://www.bsk-z.or.jp