2

ナショナル・クライシスマネジメント
危機に対する国家的情報力の強化

齊藤義明

本稿では、2001年９月11日に米国で勃発した同時多発テロを題材として、危機的状況における国家レベルでの情報力、情報の技術を探る。具体的には、①米国インテリジェンスコミュニティ（諜報機関）の情報技術の実態、②官民情報共有による国家重要インフラ防護戦略の実態、③電子政府と危機対応の実態――などを分析していく。

有事における国家の対応（ナショナル・クライシスマネジメント）には、複雑に入り組んだ問題に対して、有限の時間のなかで意思決定し、矢継ぎ早に政策を起動していくことが必要である。これに効果的に対応するためには、日本においても、危機に対する国家的情報力の強化が不可欠である。

Ⅰ　試される国家的情報力

同時多発テロという前代未聞の危機に対し、米国は軍事行動だけでなく、外交、犯罪捜査、資金フロー管理、人道的支援、被災者救済、内国セキュリティ対策などの総合的な政策を展開した。複雑に利害が絡み合う世界情勢と、脅威の続発に脅える国内情勢という極めて困難な環境下にあって、国際連携を効果的に組み立て、国家機能を粛然と機能させ、国民に団結と忍耐、勇気の精神を鼓舞した。この戦略的・統合的な一連の危機対応は、いかにして可能だったのであろうか。

一般に米国には手厳しく、皮肉を交えた分析をすることが多い英国エコノミスト誌が、今回の米国の対応をみて、「国全体としてヒステリーもパニックもなかった。ムードは悲しみ、決意、一体感であり、制御された怒りであった。これは賞賛すべきである」と論じた[文献1]。普段は個性的で多様な米国民が、なぜかくも静かに精神の団結をなしえたのだろう。

こうした米国の危機対応を可能にしたの

は、数々の国際危機に関する経験や訓練、世界情勢の把握、外交・軍事力、リーダーシップ、ヒューマニズム、ボランティア精神などの要素の総合であり、もちろんただ１つの要素で説明できるものではない。だが、危機対応の過程で、「情報」がキーファクターとして果たした役割は大きい。

情報こそが、危機的事態の背景と本質を認識し、本土防衛と制裁の対応戦略を決定し、テロ撲滅に向けた国際協調の流れを作り出し、生命の不安のなかで国民が精神と行動の規律を保つために不可欠の要素であった。したがって本稿の目的は、同時多発テロを題材に、危機的状況における国家的レベルでの情報力、情報の技術を探ることにある。

ここで注目している「情報力」「情報の技術」とは、コンピュータネットワークに体化された情報技術（いわゆるIT）だけでなく、人や組織に内在する情報技術も含めて考えている。すなわち、①CIA（中央情報局）などインテリジェンスコミュニティ（諜報機関）における犯罪情報捜査、②国家的重要インフラをテロの脅威から防護するための官民の情報連携、③有事における情報メディアのあり方、④大統領やニューヨーク市長のリーダーシップ――など、危機における幅広い情報のコントロール（情報収集、分析、洞察、戦略的編集、伝達技術）を指している。

危機とは、こうした幅広い情報力が国家的・社会的レベルで試される究極の状況に他ならない。同時多発テロでは、米国が駆使した危機対応の情報力に一面で驚き、また一面で問題を感じるとともに、日米のコントラストを再認識させられた。

危機に対応した国家的情報力は幅広いテーマであるため、ここでは以下の国家的・社会的機能に焦点を絞って検討する。

第１は、同時多発テロに対する犯罪捜査と国家安全のために、危機の最前線で情報活動を展開するCIAやFBIなどのインテリジェンスコミュニティの実態である。

米国のインテリジェンスコミュニティが、同時多発テロ後の潜在的脅威の察知と警告の発令によって、国民の安全維持に果たした役割は大きい。だが他方で、「エシュロン」（英語圏５ヵ国の共同運営による地球規模の通信傍受システム）、「カーニバル」（FBIのオンライン通信傍受システム）など情報収集技術のハイテク化を進めてきたにもかかわらず、同時多発テロを事前に察知することができなかった事実は、厳粛に受け止める必要がある。この「インテリジェンスの失敗」の真の原因は何か。インテリジェンスの改革に向けた動向と課題とを探る。

第２は、「ホームランドセキュリティ」（本土防衛）の要である国家重要インフラ防護のための官民連携の実態である。

米国では、国家重要インフラ防護戦略において８つの重要インフラが指定されており、その物理面および情報面における防護が進められている。特に、近年サイバーテロの脅威が高まっており、これに対する防御が重要課題となっている。国家重要インフラ防護の核をなすISAC（情報共有分析センター）やNIPC（国家インフラ防護センター）と呼ばれる官民情報共有のメカニズムと、その課題について考察する。

第３は、危機的事態に際し、国民の安全確保や価値観・行動の規律形成に重大な影響力を持つ情報メディアの実態である。

同時多発テロでは、日米の報道を体験的

に俯瞰したときに、視点や優先順位に大きなコントラストがみられ、その違いが国民の意識形成に多大な影響を及ぼしていると感じられた。危機において報道はいかにあるべきなのか。また、災害時の情報メディアとしてインターネットの存在感が高まるなか、政府、ニュース、慈善団体などのインターネットメディアはいかに危機に対応し、真価を発揮したのだろうか。特に、勃興期にある電子政府は有効に機能したのか、テロ危機を反映して今後どう変化し、何が新たな課題となるのかを探る。

II　インテリジェンスコミュニティの情報技術

1　機密情報の統合オペレーション

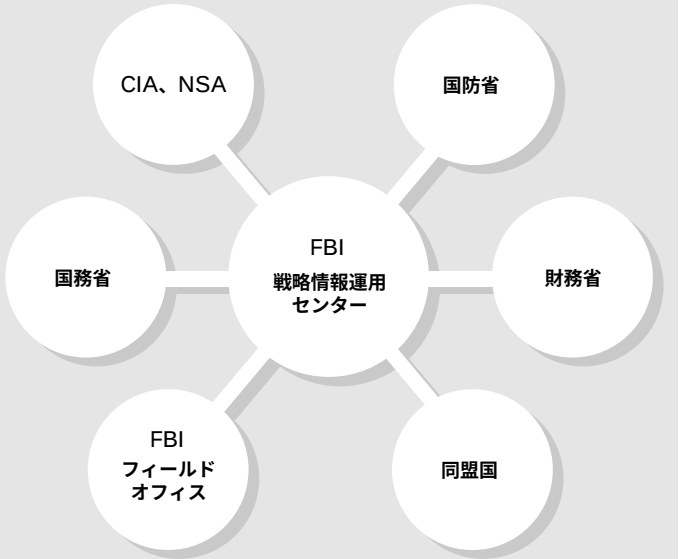
米国のインテリジェンスコミュニティを形成する各機関（CIA、FBIなど13機関）は、それぞれ異なる使命と手法を持ち、また異なる法律によって規定され、平時には権力の集中を防ぐ目的から別建てで運営されている。しかし、同時多発テロの直後から、これらの機関では犯罪捜査と本土防衛のために、組織横断的なチームワークが形づくられている。

その一例として、FBI（連邦捜査局）の戦略情報運用センター（Strategic Information Operations Center）における活動がある。このセンターには、同時多発テロ発生直後から、FBIのほか、CIA（中央情報局）、DIA（国防情報局）、NSA（国家安全保障局）、関税局などの異分野の専門官が組織を超えて参集し、全米や世界中から集まるテロ関連情報を24時間体制で収集・分析し、犯罪捜査を行っている（図１）。

約3700平方メートルのセンターの内部では、500人余りの専門家が12時間おきに二交代制で詰め、35の連邦政府組織から刻々と集められる情報の分析に当たっている。センターの環境は、さながら新聞社やテレビ局のニュースルームのようなものだといわれる。フロアは異分野の専門家数百人が密接に連携して協働できるように設計され、朝夕定期的に重要情報を共有するためのブリーフィングが行われる。

ネットワークコミュニケーションには、①標準FBIネットワーク、②トップシークレット用ネットワーク、③高度特別情報用ネットワーク――の３階層のネットワークが使い分けられており、そこにはFBIの捜査官が現場で集めた情報が時間順に整理されたうえで随時アップロードされ、全員が間違いなく最新情報にアクセスできるように制御されている。また、センターに召集された専門官が他の専門官たちと即座に情報を共有し、仕事を開始することができる

図1　FBI戦略情報運用センターにおける情報統合



注）CIA：中央情報局、 FBI：連邦捜査局、NSA：国家安全保障局
出所）ワシントン・ポスト紙、2001年10月14日（原データはFBI）

よう、「ラピッド・スタート」というグループウェアも用いられている[文献2]。

FBIの戦略情報運用センターのケース以外にも、CIAのインテリンク（Intelink）など、諜報組織間の情報共有を図るためのエクストラネットの整備が進んでいる。また、NSAの指導下で、これまで各諜報組織間でバラバラだった機密情報分類コードを統一するための改訂作業も進み始めている。

2　インテリジェンスの純度

インテリジェンスとは日本語で「情報」や「諜報」と訳されるが、ここでの意味合いはもっと深い。インテリジェンスとは、断片的な情報の集合ではない。集められた情報から、その意味や背後にある相手の意図を嗅ぎとり、政策的意思決定へとつなげる濃密な知的作業である。

インテリジェンスの純度を高めることは、実際には容易ではない。米国のインテリジェンスコミュニティには、世界中から膨大な情報が寄せられている。それらの情報は相互に矛盾する場合も少なくない。誤報はもちろんのこと、ディスインフォメーション（故意の偽情報）も混在するため、情報は錯綜する。

しかも、特定の時間内に、事態を分析して対応戦略を迅速に構築するための情報分析力が、自国の安全を守り、犯罪捜査の国際連携の効果を左右し、世界秩序の動揺を抑止するうえで極めて重要である。このため、不確かな状況下であってさえも、重要な判断をしなければならない。こうしたプレッシャーのもとでの情報収集や分析、意思決定は困難を極め、実際に同時多発テロでは狂信的集団の跳梁を許してしまったのである。

3　失敗の原因と改革の課題

（1）インテリジェンスの失敗

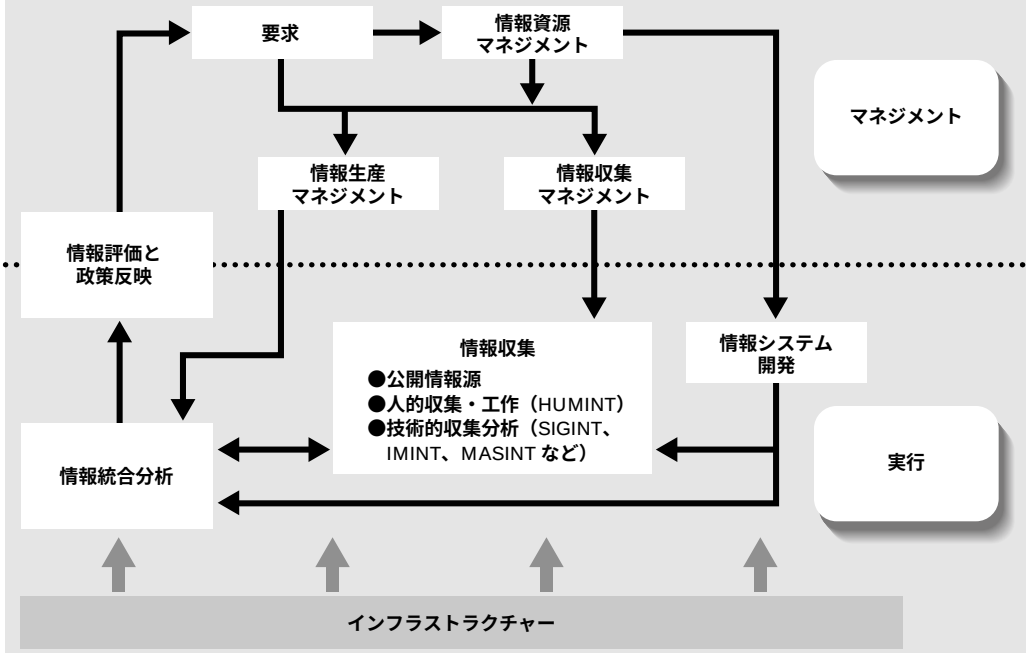
同時多発テロにおける「インテリジェンスの失敗」の原因は何か。冷戦終結後、米国はエシュロン、カーニバルなど諜報手段のハイテク化を進め、生命の危険性が高いといった人道的理由などから、生身の人間による情報収集・工作活動（HUMINT）を半減させていた。

だが、ハイテクによって得られる情報とHUMINTによって得られる情報は性質が異なる。テロに関していえば、ハイテクはテロリストのプロフィールや軍事力、交信内容などの把握に威力があるが、テロ組織が持っている内面の憎悪や考え方などはHUMINTでしか把握ができない。また、捜査手段のハイテク化に伴って犯罪手段もハイテク化するとは限らない。ハイテクの網を潜るようにして古典的手段を駆使した今回のテロ行為のように、捜査技術と犯罪技術の非対称展開が生じる。

これらのことから、犯罪企図を正確につかむためには、ハイテク情報収集だけでなく、人的情報収集・工作活動が不可欠なのである。こうした人間をツールとするハイリスクで泥臭い諜報活動からしか得られない情報や勘を欠いていたことが、今回の インテリジェンスの失敗につながったといわれている。このため現在、米国議会ではスパイ活動の自由度を拡大・強化する法案（反テロリズム法）の採択や予算化という方向に再び回帰しつつある。

また、インテリジェンスの失敗の原因は、こうした情報収集技術の問題もさることながら、集められた情報の統合的な分析技術やマネジメントの欠陥によるところが大きい。情報収集技術のハイテク化によって、

図２　インテリジェンスコミュニティの機能フロー



注）HUMINT：ヒューマンインテリジェンス、IMINT：画像解析、MASINT：科学技術的計測分析、SIGINT：通信信号解析
出所）IC21（The Intelligence Community in the 21st Century）「第104議会米国下院インテリジェンス委員会報告書」1996年6月5日

集められる情報量は膨大となったが、一方でこれらの情報を統合的に分析し、的確な対応戦略へとつなげていく方法論は依然として大きな課題である。

この点に関し、すでに1996年６月に米国下院のインテリジェンス委員会が問題点を指摘している[文献3]。同委員会の報告書では、米国のインテリジェンスコミュニティの機能を、マネジメント、実行、インフラの３層でとらえ、そのなかで情報収集、情報分析、情報システム開発、情報評価などの各機能がどう流れ、相互作用しているかを分析している。

例えば、情報収集機能を構成するものには、人による情報収集・工作活動であるヒューマンインテリジェンス（HUMINT）のほかに、通信信号解析（SIGINT）、衛星写真等の画像解析（IMINT）、科学技術的計測分析（MASINT）などの技術的情報収集が含まれる。報告によると、これらのそれぞれが組織的に分断され、独自に情報収集・分析ラインを形成しており、相互の情報統合が希薄で、すべての情報を用いた統合的分析が軽視されているという（図２）。

つまり、的確な情報分析のためには、技術間・組織間の協働が不可欠であるにもかかわらず、各組織の競合意識や縄張り争いが邪魔をして重要情報の抱え込みが起こり、統合的分析が阻まれているという大問題が、インテリジェンスコミュニティで発生している。そして、その問題はまだ十分に解決されていない可能性が高い。

例えば、CIAは他の諜報機関との間で最高機密情報を交換できるインテリンクというネットワークを開発しているが、そこに流通しているのは確定情報ばかりであり、生情報は共有されていないという実態が報告されている[文献4]。

（2）改革への３つのアプローチ

したがって、インテリジェンスの純度を高めるためには、今後３つのアプローチが必要であろう。

第１は、情報収集技術体系の改良であり、ハイテク情報収集の継続的技術開発を進めるとともに、ヒューマンインテリジェンスを強化するための人材獲得や育成、国際連携戦略の再構築が不可欠である。ヒューマンインテリジェンスの強化は長期を要するプロジェクトであり、また米国の人材だけで対応することには限界があるため、必然的に国際的な諜報連携の強化へ進むとみられる。

第２は、組織改革やBPR（ビジネスプロセス・リエンジニアリング）により、インテリジェンスコミュニティにおける情報共有や協働を促進することである。

第３は、大学や産業界と連携して、世界中の異質な文化や価値観を深く理解できる人材を戦略的に蓄積し活用することである。なぜなら、米国のインテリジェンスの失敗の１つは、米国人とは大きく異なる相手の文化や価値観、考え方を深く理解して犯罪企図を推し量る能力が、不十分であったことに起因するためである。世界中の通信内容を傍聴するテクノロジーを手に入れようとも、表面的な情報だけでは相手の行動を深く読み解くことはできない。

自分たちとは異質の文化を深く体験的に理解できる人材を備え、情報の意味を全体的な文脈のなかで分析できる体制を整える必要がある。だが、こうした人材のすべてを諜報機関内に育成することはコスト高につき、またその必要もない。大学や産業界も含めて戦略的・社会的に育成し蓄積するという国家戦略を立て、平時には国際社会を理解するためのリソースとして、また国家的危機においては情報分析のリソースとして有効活用することなどが考えられる。

III　国家重要インフラ防護のための官民情報共有

1　米国の国家重要インフラ防護戦略

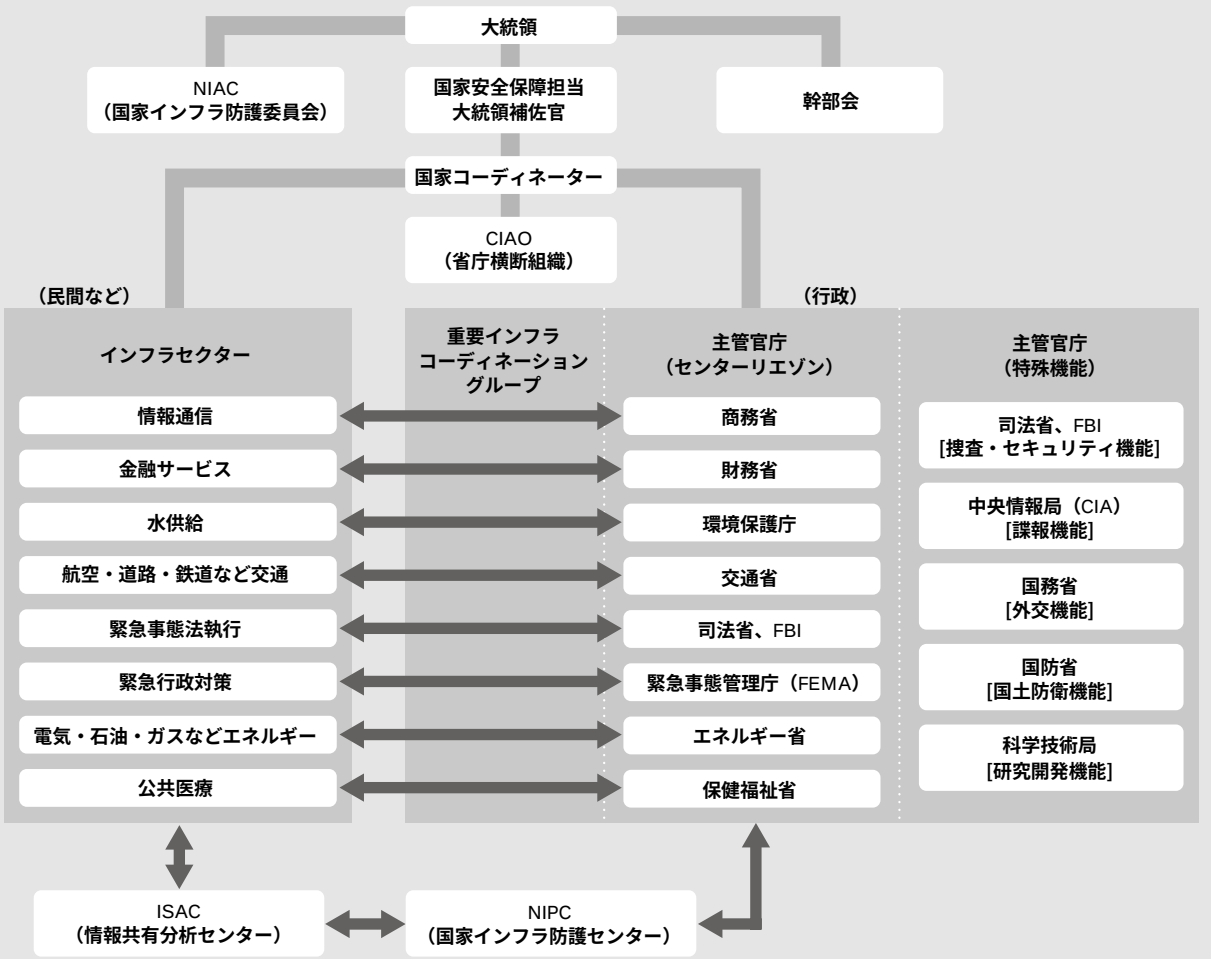
米国においては、1998年５月の大統領指令（PDD63）により、国家の基盤となる重要インフラの防護戦略が実行に移されている。そこで指定されている重要インフラとは、①情報通信、②金融サービス、③水供給、④航空・道路など交通、⑤緊急事態における捜査・法執行、⑥緊急行政対策、⑦電気・石油・ガスなどエネルギー、⑧公共医療――の８分野である。これらの物的・制度的インフラに対応する民間セクターと行政官庁とが協働し、物理的攻撃やサイバー攻撃からの防護を進めている（次ページの図３）。

この戦略体系のなかで、実務上のトップに位置するのは「国家コーディネーター」である。その担当官は、国家重要インフラ防護計画のための省庁横断組織であるCIAO（Critical Infrastructure Assurance Office：重要インフラ防護室）のスタッフを組織化するとともに、８つのインフラ防護の主管官庁（セクターリエゾン）、および諜報や国防などを司る５つの特殊機能機関と、民間セクターとの間の協力関係の構築を図っている。

2　官民情報共有のメカニズム

国家重要インフラ防護戦略においては、民間との協力関係を推進するためにISAC

図3　米国の官民連携による国家重要インフラ防護の体系



注）CIAO：重要インフラ防護室
出所）General Accounting Office, “ Critical Infrastructure Protection : Significant Challenges in Developing National Capabilities, ” April 2001（原データはPDD 63〈大統領指令63号〉）

（Information Sharing and Analysis Centers：情報共有分析センター）という情報共有のメカニズムが導入されている（図3の左下）。

ISACは、国家重要インフラに対するサイバー攻撃情報を収集・分析し、攻撃に対する防止策を検討し、それを官民のメンバー間で迅速に共有化するためのメカニズムで、各インフラごとに、民間企業メンバーと所管行政機関とから形成される。1999年10月にまず金融セクターにおいてISACが創設されたのをはじめ、2000年1月には通信セクターが、さらに2001年に入って電力セクター、情報技術セクターがISACを立ち上げている。

ISACの情報共有メカニズムの設計や運用の詳細に関する決定権限は民間セクターが持ち、また事故情報を政府に報告することは自発的であって義務ではないなど、ISACは民間主導の性格が極めて強い。このため、各ISACは多様な形態をとっている。例えば、金融ISACにおいて情報共有・分析サービスを行うのはグローバル・インテグリティ社（現在はプレディクティ

ブ・システムズ社に統合）という民間企業であるが、通信ISACの場合はナショナル・コミュニケーション・システムという省庁横断組織がこれを担っている。

また、ISACと同様の情報共有・分析のための機関として、FBIのNPIC（National Infrastructure Protection Center：国家インフラ防護センター）が組み込まれており、ISACが民間主導、NPICが行政主導という構成をとっている。NPICは、FBIの捜査機能がサイバーセキュリティ分野に特化したものであり、①コンピュータ犯罪の捜査、②分析と警告、③教育訓練と広報――の３つの役割を持つ。

3　キーアセット・イニシアチブ

このNPICが展開するプログラムのなかに、国家重要インフラのなかでも中核をなす資産について、民間企業の所有分も含めて詳細に把握し、データベース化する「キーアセット・イニシアチブ」と呼ぶ注目すべき活動がある。85%以上が民間所有といわれる国家重要インフラの具体的資産状況を事前に把握しておくことは、各施設や設備に対する攻撃の潜在的な影響を事前に評価し対策を講じるうえで重要な意義を持つ。これにより過小防護や過大防護といった戦略ミスを避けることができる。

NIPCのマニュアルによると、８つのインフラセクターを構成する主要資産について徹底的な調査と確認を行い、これらの重要性を、全国的に影響が及ぶものから局所的な影響にとどまるものまでに格付けし、その情報に基づいてインフラ所有者の危機管理計画を支援する、という基本手順が示されている。この調査によって、実際に全米で5000以上の主要インフラ資産が特定されている。

ただし、GAO（米国議会の政策評価機関）がその後にこれを追跡調査した結果によると、このデータベースは必ずしも十分な信頼性を持っていないようだ。なぜなら、調査の過程で調査員が独自の判断により故意に除外した資産があること、調査地域によって調査精度の濃淡が大きすぎること、情報源として電話帳を使うといった怠慢があることなどによる[文献5]。

4　官民情報共有化の課題

以上みてきた、国家重要インフラ防護のための官民情報共有の戦略的・組織的な取り組みは、①国家重要インフラに対するサイバー攻撃の防止策を迅速に検討し、その影響を最小限に抑える、②犯罪捜査を効果的に進める、③各組織におけるサイバー攻撃のリスク意識を高め、リスク評価を助ける――などの観点から極めて重要であり、今後日本の危機管理においても注目していくべき仕組みといえる。

しかし米国でも、いくつかの理由から、こうした情報共有は必ずしも理想的には進んでいない。官と民との間で十分な信頼関係が構築されているとはいえず、情報共有が一部で阻害されているためである。すなわち、官は、国防上の理由から、サイバー事故にかかわるデータを未公開、あるいは修正したうえで民間メンバーに公開することがあり、これは情報の有用性を低めるとともに、処理時間を長期化させている。

また民は、法令遵守違反を指摘されることを恐れ、官（司法省など）に事故情報を提供することを躊躇する場合がある。さらに官と民とでは、そもそも情報セキュリティに対する許容リスクの範囲やコスト負担

意識に乖離があり、この点も協調関係を困難にしている。一方、民同士でも、競合他社が自社の事故情報を漏洩することによって企業イメージが大きく損なわれるリスクがあるため、ISACに報告をしない企業がある、といった問題を抱えている。

ISAC（民間主導）とNPIC（FBI主導）間の情報共有についても、NPIC（官）からISAC（民）への情報の一方通行といわれており、ISAC（民）の情報がNPIC（官）に提供されていないことも、国家インフラ防護上無視できない課題である。

したがって、実効性の高い国家インフラ防護策を確立するためには、まず官民情報共有のメカニズムを構築することが第一歩となる。加えて、一定のレベルを超えた事故情報はすべてその情報を共有することを義務づけるなど、官民間の運用基準を明確化し、また意図的情報流出に対してはこれを厳しく罰する法的措置を講じるなど、情報共有の実効性を高めるための環境整備が必要であろう。

Ⅳ　情報メディアと電子政府の危機対応力

1　危機報道の日米差

同時多発テロの発生後、人々は真っ先に情報を求めた。これに対し、迅速で的確な情報提供によって社会的パニックが抑制され、その後も国民の団結やテロにひるまない精神態度が形成されていった。先のエコノミスト誌は次のように伝えている。

「もしテロリストが広範なパニックの引き金を引こうとしたのなら、彼らは失敗した。全く逆のことが起こったのだ。ニューヨークは恐怖の挑戦に対して立ち上がった。タクシードライバーはシートを剥ぎ取って爆心地から犠牲者を運んだ。数十万人のワーカーは落ち着いてダウンタウンから歩いて脱出した。（中略）多くの人々が献血を申し出、追い返されるほどだった」[文献6]

こうした国民の精神や行動の規律形成に及ぼすマスメディアの影響力は大きい。同時多発テロへの対応の過程では、日米の報道姿勢の違いを目の当たりにした。

日本の報道がまず邦人の安否、そして経済への影響に偏る一方で、米国の報道は状況理解、事態の定義、対応と決意、戦略と戦術などを、優先順位の確かな意識を持って伝えていた。米国では死傷者情報の伝達にはテレビではなく、インターネットが利用されていた。米国の報道には、突発的な事件であってさえ、問題を扱うときの確かな構造があり、議論の優先度が意識されており、現役や前職の専門家を交えて多岐にわたる議論が展開された。

また、事件後数ヵ月が経過しても、米国では本事件にかかわる犯罪追跡、戦局、潜在的脅威と対策、法律や予算面での対応、さらに事件の本質をえぐる報道などが中心であり続けた。他方、ダイジェスト版でみる日本のテレビニュースにおけるテロ危機の扱いは、時が経つにつれ周辺的なものへと推移し、その内容も問題解決のための主体的議論や分析というよりは、解説的な態度であった。

これは米国が同時多発テロの当事国であり、日本が非当事国だから、事件の持つ重みが違うということなのだろうか。それとも、メディアが国民の精神・意識の質の高さを映し出す鏡であるとすれば、これはわれわれ日本人の問題意識の希薄さの反映な

のであろうか。筆者の観察は、同時多発テロ以後の日米のテレビや新聞に接して抱いた印象論にすぎない。しかし、日米メディアの報道の視点や分析力の違いに問題意識を持っている者は少数ではない。

よく、報道の質を評価する際に「客観性」や「バランス」という基準が用いられる。今回の米国の報道は、政府のプロパガンダのようであり、バランスを欠いていたとの批判がある。確かに、米国の政府・メディア・国民は共鳴し団結していた。だがそれは、この国が普段はバラバラで多様な意見をもつ国家であるだけに、意識的に結束することが必要だったからである。この危機的状況に対し何が必要なのかを、それぞれが感じとっていたからである。

危機的状況においてさえ、視点の多様性やメディアの自律性を保つことの重要性は否定しない。だが、有限の時間のなかで明確な意思決定が不可欠であるとき、議論を発散させ、批判に終始するだけでは、何も解決しないのが現実である。日本の報道には、概して、問題を分析していく大きな「構造」、いま何が重要なのかを判断する「優先順位」、有事において平時のような発散した議論をしない「時局観」が欠けているように思われた。

マスコミに限らず、情報の受け手であるわれわれ自身も含めて、国際的危機に対し当事者意識を持って対処する意識や知的訓練を積み重ねることが必要である。これは長期的な日本の人材育成の課題である。

2　危機的状況におけるインターネットメディアの価値

災害時の情報メディアとして、テレビ、新聞、ラジオだけでなく、インターネットの存在感が高まっている。すでに阪神大震災のときからインターネットの潜在力は高く評価されていたが、あれから７年を経過し、インターネットはさらに普及成長を遂げ、今や必須の情報メディアとなった。それだけに、同時多発テロがインターネットメディアに及ぼした影響はいっそう本格的なものであった（表１）。

同時多発テロ発生後、ABCNews.com、MSNBC.com、CNN.com、NYTimes.com（いずれもマスコミ）などのニュースサイト、FBI.gov、CIA.gov、SEC.gov（証券取引委員会）などの政府機関サイト、AA.com（アメリカン航空）などの航空会

表1　主要ウェブサイトのダウンと回復過程

9月11日	
午前9時過ぎ	**世界貿易センタービルへの最初の航空機激突の報道** ●CNN.com、ABCNews.com、NYTimes.com（いずれもマスコミ）が利用不能化 ●USToday.com、MSNBC.com（いずれもマスコミ）の利用可能率がそれぞれ18%、22%に低下
午前10時	**同時多発テロ攻撃の詳細報道** ●FBI.gov（連邦捜査局）が以後12時間利用不能化 ●SEC.gov（証券取引委員会）が2時間の停電
午前11時	**ハイジャック航空機の特定に関する報道** ●AA.com（アメリカン航空）が以後6時間利用不能化 ●UAL.com（ユナイテッド航空）の利用可能率が深刻な低下
正午～深夜	**航空機攻撃の沈静化報道** ●CNN.com、ABCNews.comが回復 ●NYTimes.comは依然としてダウン ●SEC.govが回復 ●FBI.govが87%の利用可能率に回復 ●AA.comが部分的に回復 ●CIA.gov（中央情報局）、FAA.gov（航空局）、FEMA.gov（緊急事態管理庁）のパフォーマンスが低下
9月12日	**同時多発テロの被害状況報道** ●FAA.govの応答時間が104秒に低下 ●FEMA.govの応答時間が25秒に低下
9月13、14日	**多くの旅行者が帰路へ** ●AA.com、UAL.comのパフォーマンスが低下 ●NYTimes.comの応答時間は依然50～100秒
9月17日	**ニューヨーク株式市場再開** ●Datak.com、Webstreet.com（いずれもインターネット証券）の利用可能率が70%以下に低下 ●CIA.govの利用可能率が66%に低下、応答時間も70秒 ●DoD.gov（国防省）の応答時間が9.2秒に低下

出所）米国キーノート・システムズ社の資料（2001年9月25日）より作成

社サイト、RedCross.org（赤十字）などの慈善活動団体サイトではアクセス数が急増した。例えば、MSNBC.comでは、平時のビジター数300万から事件後平均900万に上昇し、最高時2000万を記録した。また、RedCross.orgでは、平時の５万ビジターから250万ビジターに上昇し、オンライン募金額も1000ドル程度から100万ドルに急増した。

このため、これらのサイトのアクセス容量は深刻な打撃を受け、CNN.com、ABCNews.com、NYTimes.comでは、一時全く利用できない状態に陥った。いくつかのサイトは完全停止こそ免れたが、応答時間が数十秒から数分というイライラするほど長いものとなった。

だが、緊急事態への対応も早かった。ニュースサイトにおいては、系列サイトからアクセス容量を緊急調達し、またグラフィック機能、広告、パーソナライズ機能を削ぎ落として減量化を図り、さらにコンテンツを緊急情報に絞り込むなどの処置がとられた。赤十字などのボランティア組織にはこうした系列調達は不可能であるため、Yahoo.com（ヤフー）やAmazon.com（アマゾン）に支援を仰ぎ、オンライン募金のトランザクション機能を暫定的に引き継いでもらうなどの協力関係が構築された[文献7]。

有事における個人のインターネットメディアの利用方法という点でも、テレビ、新聞との補完関係が明確になってきたようだ。つまり、時々刻々と変化するニュース速報はテレビやラジオが主力メディアであり続けたが、分析や洞察という点では新聞（特にワシントン・ポスト紙やニューヨーク・タイムズ紙）が長けており、情報検索や必要情報にいつでもアクセスできる点でインターネットが極めて重要なメディアであった。

特に、事件の経過につれ、ある者は炭疽菌関連情報、またある者は航空機の運行情報など、人々の関心事が多様化してくると、限られた時間枠や紙面枠に限界を有するテレビ・新聞ではあらゆる関心への全方位対応が困難となる。しかしインターネットは、情報が広角的で重量化するにつれ、各人のニーズに応じた深い情報入手ができる点で、その真価を発揮していった。

またインターネットは、重要人物の演説や発表内容の原テキストを入手することが容易であるため、マスコミが選別した視点や情報に流されずに、自ら情報を編集し判断しようとする者にとって重要な情報源となった。さらに、マスコミとは別の世界で、同時多発テロの意味を考え、意見の形成や交換を行うメーリングリストが数多く立ち上がり、草の根的な議論が展開されていったことも無視できない。

こうした「主体的判断のためのインターネットメディア」活用の流れは、マスメディアの情報に受動的に反応するだけでなく、自ら情報を吟味し、当事者意識を持って考え抜く人間の形成のために、重要な意味を持つと考えられる。

3　電子政府と危機対応

（1）危機に対する初動

危機におけるインターネットメディアの重要性が高まるなか、政府の情報ゲートウェイとして電子政府の対応も注目された。米国連邦政府のワンストップ情報ポータル「ファースト・ゴブ」（FirstGov）は、テロ事件発生後にヒット数が1.5倍以上、ビジター数が２倍以上、１回当たり平均アクセス

時間が４倍以上に上昇した。

ファースト・ゴブが緊急事態に対応した情報ページを最初に掲載したのは、９月12日、事件発生から丸１日が経過してのことである。個人のボランティアがいち早く世界貿易センタービルの生存者リストを掲載したのが事件発生から１時間30分後といわれており、こうした先駆的個人の対応には及ばないものの、通常の官僚的対応に比べるとファースト・ゴブの対応は早かったといえる。ペンタゴンが攻撃を受け、連邦政府ビルからの職員の退去避難令が出されるなか、ファースト・ゴブの担当チームは在宅作業も行って緊急情報ページの立ち上げを始めた。

ファースト・ゴブは連邦政府の4700万サイトの情報を統合するサイトであり、通常は各サイトの更新情報をチェックするだけでも４日間が必要という。このため以前は２週間ごとにコンテンツを更新していたが、同時多発テロ発生後は、チェックすべきサイト数を絞り込み、12時間ごとに情報更新する方式に切り替えた。

同時多発テロに直面し、ファースト・ゴブ担当チームがまずすべきことは、標準サイトのなかに緊急情報ページを立ち上げ、危機対応の情報リンクを形成することであった。しかし、やみくもなリンク形成はかえって混乱を引き起こしかねない。彼らはリンク先のトラフィック処理能力を確認し、必要なリンク形成を冷静に判断した。ファースト・ゴブを知らない米国民に対しても広く情報アクセスを提供するために、民間ポータルやニュースサイトとの緊急提携も行った。

また、事件後の日々の状況変化のなかで、国民の情報ニーズを的確に判断し、情報提供内容に反映することが重要であった。当初は「人探し」を緊急情報ページのトップに掲載していたが、数週間後には死亡者・行方不明者に対する支援施策情報中心に切り替えるなど、状況に応じて編集の焦点を移動していった。さらに、事件の推移に伴って情報量が増大するなかで、情報カテゴリーの分割を適宜実施していった[文献8]。

電子政府の認知度や利用率は、テレビ、新聞などのマスメディアに比べるとまだまだ低いものの、有事の情報源として重要な役割を担いつつある。ファースト・ゴブが同時多発テロの最中にとった行動、すなわち、緊急情報ページの立ち上げにおける冷静かつ起業家的な判断と行動、時々刻々と変化する国民の情報ニーズに対する編集政策、アクセスを拡大するための民間ポータルとの緊急提携などから、日本の電子政府が学び、備えておくべきことは多い。

日本の電子政府はいま勃興期にあり、システム構築の方に眼を奪われ、運用面で必要な課題に対してまだ十分な注意が向いていない。今後は、危機対応を含む運用面でのシミュレーションと備えにも注目が必要であろう。

（２）米国電子政府の中期的変容と課題

中期的にはテロ危機を反映して、米国の電子政府は大幅な転換を迎える可能性が生じている。ブッシュ大統領の政治任命によりサイバーセキュリティ担当大統領特別補佐官に就任したリチャード・クラーク氏は、2001年10月、サイバー攻撃に強い政府専用のネットワークの整備構想を発表した（次ページの表２）。これは「ゴブネット」と呼ばれ、インターネットと一切接続せず、政府と許可された関係者のみにユーザーを

表2 「ゴブネット」基本構想

- **IP（インターネットプロトコル）接続方式を利用し、政府機関と許可されたユーザーのみが情報を共有する**
- **インターネットその他の公開・民間ネットワークとは一切の接続やゲートウェイを有しない**
- **全米48州をイントラネットで結ぶ**
- **遠隔会議や放送などのため、音声コミュニケーション（商用レベル）を可能にする。また、現段階では必ずしも要求しないが、今後映像コミュニケーションが付加できるようにする**
- **サイバーアタック、サービス拒否攻撃（DSA）、コンピュータウイルスなどの悪意のある破壊・妨害行為が不可能なものとする**
- **トラブル発生時の迅速な復旧など、最高度の信頼性と利用可能性を持つ**
- **NSA（国家安全保障局）認定の暗号技術を用いるなどして、情報伝達の安全性を確保する**
- **民間が開発し、政府などユーザーにサービス料を課金するといった、柔軟なビジネスモデルを認める**
- **すべての装置やリンクは米国内またはカナダ内に設置されなければならない**
- **24時間無休で運営される**
- **契約後6ヵ月以内に指定された政府機関をネットワーク接続し、サービスを開始する。また、12ヵ月以内に音声と画像通信を加える**
- **伝送装置・ルーター・ネットワーク制御装置などすべてのハードウェア構成の専用整備や、ネットワーク管理・運営にかかわるすべてのスタッフの専任化も1つの案として見込む**

出所）GSA（米連邦調達局）「ゴブネット開発に関する民間からの提案募集」2001年10月10日

限定した非公開ネットワークである。オープンネットワークであるインターネットが内在するサイバー攻撃に対する脆弱性をシャットアウトしようとの考えである。

電子政府の展開において、インターネットに対する不信感がこれほど明確に示されたのは初めてである。この新しい流れが、今後どの程度本格化するかは明確ではない。だが、今後世界的にテロ危機の解決が長引くならば、広範な行政情報が非公開情報となる流れが生じることが懸念される。実際、同時多発テロ以降のセキュリティ強化のなかで、テロ活動に悪用される可能性があるとされるいくつかの情報（核反応炉、化学プラント、燃料パイプライン、防護オペレーションなど）が政府サイトから消し去られている。

電子政府は、開かれた情報ネットワークをベースに行政改革を追求するものであり、その進捗や成果を国民が実感し判定することができるという点で優れている。このインターネットベース改革ともいうべき流れが、安全や国防上の理由で減速を余儀なくされ、非公開ネットワークのもとで行革努力がなおざりにされたり、安全を理由に行政プロセスが複雑化し組織が肥大化したりすることに対して、十分な注意が必要である。安全を隠れ蓑に行革の停滞を許すことがあってはならない。

V　国家的情報力強化の必要性

本稿では、米国での同時多発テロの体験・観察を通じて、国家的危機管理という重大かつ広範囲に及ぶ問題の核心の１つは「情報力」であるととらえ、その強化の必要性と基本的方向性を探った。分析に際しては、情報力を狭義のITだけでとらえずに、ITと個人や組織が織りなす総合的な情報の技術としてとらえた。また、米国の危機対応システムの優れた着眼や先進的取り組みを鵜呑みにせず、その課題をも照射するよう努めた。

国家的危機対応の戦略や手法、技術について研究しなければならないことはまだまだ多く、本稿はその一部をなすにすぎない。ここでは主にインテリジェンスコミュニティの情報技術の実態、国家重要インフラ防護戦略の実態、電子政府と危機対応の実態などを分析したが、これら以外にも日本にとって対策が急がれる分野は広がっている。例えば、生物・化学テロ危機に対する諸機能整備の重要性、緊急性である。生物・化学テロの脅威が米国民の精神に与えた影響は大きく、社会的パニックがいつ起こっても不思議ではなかった。

また、より大きな構図からみると、一国の危機対応力は、個々人のセキュリティアクション、企業の危機管理・事業継続化計画（コーポレート・クライシスマネジメント）、国家的な危機対応戦略（ナショナル・クライスマネジメント）などの重層構造をなしており、それぞれについての研究や各層の相互作用の分析が重要課題として残されている。

加えて、国際的脅威が固定的・静的なものから、流動的・可変的・ネットワーク的なものへと変質しており、その対応についても状況に応じた地球規模の連携が必要になっていることを考えると、これからの危機対応には国際連携の視点が欠かせない。いずれも、日本では着手・見直しが不可欠の重要課題といえる。

有事における国家の対応は、複雑に入り組んだ問題に対し、有限の時間のなかで意思決定し、矢継ぎ早に政策を起動していくことが不可欠である。これに効果的に対応するためには、大統領、首相などのリーダーシップはもとより、米国のインテリジェンスコミュニティにみられたようなリーダーの意思決定を支える情報オペレーション、国家重要インフラ防護戦略にみられたような官民情報共有のメカニズムが、日本でも整備・強化される必要がある。

根本的には、国家的な情報機能強化だけでなく、国民一人一人が世界情勢に対する現実的な洞察力を養う教育の改革が必要である。少なくとも関連官庁や情報産業に携わる者は、情報の収集、分析、洞察、戦略的編集、伝達などに関し、再度、能力向上に努める必要がある。

同時多発テロに限らず、多様な国際的危機の原因が現在の世界システムの歪みから生み出されているのだとすれば、危機はこの先偶然に起こるのではなく、構造的・必然的に潜在し、予測は不可能なものの、勃発の危険性はすぐそこにあるという状態にわれわれは置かれている。この世界の裂け目を事前に回避・予防する国際協力と、これが生じた場合の危機対応の強化は、今後避けて通れない道である。

完全に平和でリスクのない世界はこの先もないとの現実的な覚悟をし、そのうえでリスクをとっていく国家・国民の態度と、備えとしての国家的危機対応技術、情報力の強化が不可欠である。

参考文献

1 “The Day the World changed,” *Economist*, Sept. 15, 2001
2 “In Federal Law Enforcement, ‘All the Walls Are Down’” *Washington Post*, Oct. 14, 2001
3 IC21（The Intelligence Community in the 21st Century）「第104議会米国下院インテリジェンス委員会報告書」1996年6月5日
4 “The Intelligence Test,” *National Journal*, Dec. 1, 2001
5 General Accounting Office, “Critical Infrastructure Protection: Significant Challenges in Developing National Capabilities,” April 2001
6 “No surrender,” *Economist*, Sept. 15, 2001
7 “Site Operators Regroup: News, Government, Charity sites toss out old assumptions as new thresholds,” *InternetWeek*, Sept. 24, 2001
8 “FirstGov Handles Millions of Web Hits After Attacks,” *Government Computer News*, Oct. 8, 2001

著者

齊藤義明（さいとうよしあき）
NRIアメリカ・ワシントン支店バイスプレジデント
専門は社会経済構造改革