Management Journal
MJ, 4: 81–98(2011)
Received 14th November, 2012

新たな脅威に対するリスクマネジメントシステムの整備と展開

Preparation and Development of Risk Management Systems for Forthcoming Threats

関西大学 羽 原 敬 二

Kansai University
Keiji HABARAI

要旨

今後の危険事情（ハザード）の変化を踏まえ，将来にわたり大きな脅威として想定される事象の中から重要な課題として，①地球規模の災害リスクマネジメントとしての小惑星衝突リスクマネジメントと感染症リスクマネジメント，②海洋の安全保障，領海警備，および有事への対応にかかわる海事危機管理システムの構築，③インフラの維持・管理としてのアセット・リスクマネジメント，④サイバー攻撃に対抗するリスクマネジメントシステムの構築，⑤資源・エネルギー確保におけるリスクマネジメント，にかかわる問題を選択して取り上げ，脅威から生じるリスクの実態を把握すると共に，具体的にどのような対策が有効または必要とされるのかについて論じた。これまでに認識されていなかったリスクに対して，新たに構築すべきリスクマネジメントシステムの構成と内容を考察することによって，これからの安全・安心な社会の形成・確保に必要となる条件を明らかにした。

Abstract

Considering the volatility of forthcoming hazards, ① asteroid impact risk management and pandemic risk management in the global catastrophic disaster risk management, ② maritime crisis management to deal with maritime security, territorial water defense, and a state of emergency, ③ asset risk management in the maintenance of infrastructure, ④ cyber risk management system, and ⑤ natural resource and energy risk management are selected among critical issues on predictable events in the future and identified in terms of risks arising from threats, examining the effective or necessary measures taken against them. The fundamental requirements to ensure the safe and secure society from now on are clarified by analyzing the contents and structures to newly establish risk management systems against risks insufficiently recognized.

キーワード　リスクマネジメント , セキュリティ，海事 , 危機管理，インフラ

Key Words　risk management, security, maritime, crisis management, infrastructure

はじめに

リスクマネジメントには，大きく分けて，国家，地域，多国間，国際関係等に関するリスクを対象とするマクロリスクマネジメントと企業，事業者団体，家庭，個人等のリスクを取り扱うミクロリスクマネジメントがある。リスクマネジメントの下位概念である危機管理も，事態処理の緊急度が高く，解決・対処の迅速性が求められている問題であって，直面しているリスクに関しては同様の対応が必要なものである。したがって，マクロ危機管理とミクロ危機管理が考えられる。

現在は，地球規模のハザード（潜在的危険事情）の増大により，リスクそのものが多様化，複雑化，国際化，巨大化，複合化，連結化，社会化しつつ変化しており，それに応じて，リスクマネジメントも個別分野別，部門別，領域別の本質的・具体的なリスクマネジメントシステムとして展開すると共に，従来よりもさらに総合的なリスクマネジメントシステム思考が求められる状況に置かれている。わが国では，防災対策，医療制度，公衆衛生管理，安全管理，環境管理などのリスク処理問題は，自然科学，医学，工学，社会・人文科学等の個別分野ごとに研究されてきたが，高度産業技術社会をむかえて，学際的かつ国際的な視野を持ったリスクマネジメントの必要性が認識されている。

一方，我々が生活しているこの地球社会は，グローバリゼーションによりますます複雑に相互依存関係を強めており，現在の成長を支えている様々なシステムを維持・管理する能力や安全性が劣化しつつある現象もみられる。たとえば，新規開発技術，金融市場の相互依存関係，資源の枯渇，少子高齢化，および気候変動などから生じるリスクによって，これまで安全・安心な社会を確保・維持するシステムとして機能してきた政策，基準，規範，または構造物・機械設備などの脆弱性や不安定性が一部で表れ出している。今まで安全・確実であったシステムが，もはや将来にわたっては，必ずしも適切に機能し続けるとは限らない時代に突入したともいえる。[1)]

そこで，本稿では，現在想定されている今そこにある危機または迫り来る脅威や大規模なリスクの中から，わが国にとって，社会的インパクトの大きいもの，より重要度の高いもの，または処理すべき緊急度の高いものを取り上げて，どのように必要な措置または方法をとることが求められているのか，新たなる脅威に対して構築すべきリスクマネジメントシステムの課題を論じることとした。

なお，東日本大震災（東北地方太平洋沖地震）に関し，この未曾有の大震災によってわが国が直面している危機的な状況，復旧対応から長期的な復興事業に至る各種の重要な問題については，未だ全体として把握・認識が不十分な点が多く，物的資産の処理，生産活動の落ち込み，電力供給不足，福島原子力発電所の事故処理などを含め，一層大きな経済的悪影響が拡大する可能性を考慮しなければならず，現時点では継続的に調査中のため，今後の課題として，本考察からは除外することとした。

１．地球規模の災害リスクマネジメントシステム

1−1．小惑星衝突リスクマネジメント[2)]

隕石による津波は，その発生頻度は極めて低いが，他の原因による津波の規模をはるかに超えるものであり，甚大な被害が発生する可能性がある。典型的な事例は，6,500 万年前の白亜紀末期に K/T-Impact と呼ばれる隕石衝突により発生した津波である。この隕石衝突は，恐竜を含めた地球上の生命体の絶滅をもたらしたとされる。隕石落下時の衝突エネルギーおよびクレーター形成後に周辺から流入する海水により生じる津波があり，発生領域や広域への伝搬シミュレーションがなされている。

小惑星（asteroid）が地球に接近し，地球の

全軌道面積に対する衝突断面積を考慮に入れると，衝突確率は，次のように推定されている。

- 直径 10km － 1 億年に 1 回
- 直径 1km － 数十万年に 1 回
- 直径 100m － 数百年に 1 回
- 直径 10m － 1 年程度で 1 回

音速以下で物体が地球に衝突しても，実際に衝突した部分以外ではほとんど影響がないが，超音速では爆発が起きる。衝突場所が陸地でも海面でも，爆発現象にはほとんど違いがなく，衝突物体の直径の数倍に及ぶ高さまで岩石や海水が吹き上げられ，海洋では，巨大津波が発生する。

直径 1km の小惑星が超音速で海面に衝突すると，直径の約 20 倍，20km の範囲で深さ数 km も海水が吹き上げられて，1,000km の広い範囲に撒き散らされ，一部は直ぐに落下するが，残りは成層圏まで達して，微小な氷粒の雲となり，全地球規模で拡散していく。氷粒や塵粒は，太陽の光を吸収・散乱して太陽光がほとんど地表に到達しなくなるため，全世界的に平均気温が摂氏 20 度から 30 度低下すると推定されている。結果的には，植物が育たなくなり，食物不足によって多くの生命種が絶滅の危機に陥ることになる。

したがって，最も大きな要件は，太陽光を遮る粒子が成層圏にどれだけ吹き上げられ，どのくらいの期間落下しないで滞留しているかである。全地球的規模での災害をもたらす衝突小惑星の規模は，衝突場所や小惑星の組成など種々の不確定要素はあるが，直径 1km が一応の境界であるとされる。かくして，小惑星衝突は，人類絶滅をもたらす潜在的な可能性をもつ事象である。

なお，津波は，歴史的にはそのほとんどが地震起源による災害とされるが，小惑星衝突起源のものも含まれていると考えられる。今後の対策上，2 種類の津波の原因を区別または認識する方法を開発することが求められる。

小惑星衝突リスクを回避する方法は，危険な衝突可能天体を発見し，軌道を決定することである。すなわち，当該天体の性質として，いつどこに衝突するかを明らかにすることにより，衝突回避のための対処法を実施することが可能となる。

1-2. 感染症リスクマネジメント[3)]

広義の健康危機管理は，感染症の大規模発生など健康に直接かかわる事象に起因する狭義の健康危機（health crisis）と，自然災害（natural disaster； 地震，津波，火山噴火，風水害等）および人為的災害（man-made disaster; テロリズム，化学・放射性物質事故等）に伴って発生する間接的な健康上の問題を指す健康関連危機（health-related crisis）に分類され，重篤な健康危機は，社会や環境に負の影響を及ぼす災害（disaster）の一種とみなされる。緊急事態が発生した場合に，被害を最小限にとどめる対処行動である健康危機管理は，医薬品，食中毒，感染症，飲料水，その他の原因により生じる国民の生命，健康の安全を脅かす事態に対する健康被害の発生予防，拡大防止，治療等に関する業務と規定されている（平成 13 年厚生労働省健康危機管理基本方針）。

感染症は，曖昧に始まり，突然に気付かれることが特徴である。感染症は，①感染源（感染源となる病原微生物の存在），②感染経路（病原微生物が宿主内に入る経路），③宿主（病原微生物が増殖する宿主），によって成り立つ事象である。感染症の危機は，これらの 3 要素が揃い，潜伏期を経た後に，宿主が発症することでしか把握できない。この時点では，既に感染源である病原微生物が量的にも空間的にも拡大し，新たな感染の危機が始まっている。

感染症の未然防止または感染症発生後の抑止方法は，宿主が免疫を獲得することしかない。しかしながら，病原性微生物すべてのワクチンを準備し，発症に応じて接種することはできず，病原性微生物は，抗原性を巧妙に変化させることによりワクチンの阻止効果から逃れるものもある。すなわち，すべての感染症を未然防止す

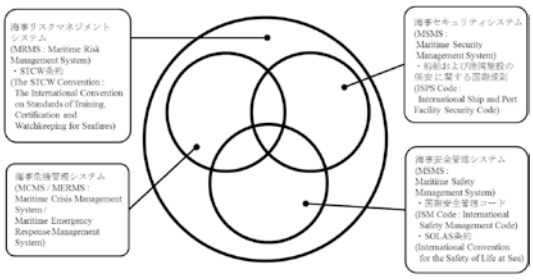
ることは絶対に不可能であることを前提としなければならない。感染症対策は，伝播予防することにより，他者の発生を抑制できることである。したがって，感染症の戦略的危機管理は，個人の感染症発生を抑制することではなく，感染症を早期に把握して，地域流行を最小限に抑えることをいう。

未知のウイルスや細菌から国民の生命を守るには，状況に応じて専門家の判断に基づいた素早い意思決定ができる仕組みが必要である。そのためには，危機管理の視点に立った感染症のサーベイランスを日常的に行うことが最も必要な措置である。感染症の危機管理におけるサーベイランスの目的は，危機の拡大を抑制するための行動を起こす契機を得ることにある。重要な要件は，迅速性であって，正確性ではないことを十二分に認識すべきである。

なお、毒性の強い鳥インフルエンザウイルスのワクチン研究については、テロリストによる研究成果の悪用を予防するバイオテロリズム対策が不可欠となる。

2. 海事危機管理システムの構築とリスクマネジメントシステム [4)]

図１　海事リスクマネジメントシステムの構造



（筆者作成）
（注記）この構図は、他の分野におけるリスクマネジメントシステム構築にも基本的に適用できる。

2-1. 領海侵犯への対応と領域警備法の制定

現在の日本には，領海侵犯を取り締まる法律がない。すなわち，領域警備法，領海法，または領海警備法がなく，したがって，領海侵犯罪もない。そのため，領海侵犯という国家主権を侵害する不法行為を犯罪として取り締まるために，漁業法，出入国管理，および難民認定法，または覚醒剤取締法などで対処しているのが実情である。尖閣諸島沖における中国漁船のように，悪質な公務執行妨害，往来危険罪，および海上交通安全法違反である場合には，国際法上では，巡視船に体当たりしてきた時点で，銃砲撃を受けてもやむをえないとされるが，日本の巡視船は銃砲撃ができない。

日本では，領域警備法，領海法，または領海警備法がないため，日本の領海を侵犯しても罪に問われない。外国漁船が日本の領海内で操業しても，魚業法違反の密漁により罰金刑の微罪で取り締まるしか方法がない。不法侵入者が暴れた場合には，公務執行妨害で逮捕するしか方法がない。もし発砲する場合には，刑法 36 条の正当防衛，および 37 条の緊急避難を適用することになっているため，現在は相手が撃ってこない限り，こちらからは射撃できない。したがって，武装勢力が発砲せずに上陸してきた場合には，海上保安庁も海上自衛隊も対処できない事態が発生することになる。

領域警備法が整備されれば，刑法 35 条正当業務行為の援用が可能になる。すなわち，領域警備法に基づく国家主権の行使として，侵略者または侵入者に対して警告射撃または船体射撃が可能となる。

2-2. 武器使用規定の制定

現在の日本の安全保障体系においては，海上の治安が、海上保安庁の警備力では治安を維持することが困難となった場合に，防衛大臣が内閣総理大臣の許可を得て，海上警備行動（自衛隊法 82 条）を発令すると，陸・海・空の 3 自衛隊は，海上保安庁を支援して武器を使用する

ことができる。これは，自衛隊法第 76 条の防衛出動における武力の行使とは法律上区別される警察力の行使である。

武器の使用は，自衛隊法第 78 条命令による治安出動，同法第 81 条要請による治安出動，同法第 95 条武器等の防護のための武器の使用，同法第 95 条の 2 自衛隊の施設の警護のための武器の使用による 2 つの要件と 4 つの条文で規定されている権限である。いずれも防衛行動ではない警察行動であり，警察官職務執行法第 7 条の準用として許されている行為である。

したがって，刑法第 36 条正当防衛および刑法第 37 条緊急避難の場合に限り，人に危害を与えてよいのは，死刑・無期，または長期 3 年以上の懲役または禁錮にあたる凶悪な罪を犯した者の逃亡防止または抵抗抑止という要件で規制されている。つまり，密漁による漁業法違反やジグザグ航法による海上交通安全法違反程度の軽い犯罪では，海上自衛隊は，警察および海上保安庁と同様に武器を使用できない。仮に，違法行為を犯した者を銃砲撃して射殺した場合には，警察比例の原則に反する過剰警備となり，特別公務員暴行陵虐罪，傷害罪，または殺人罪として訴追され，刑事罰を受けることになる。

海上で局地的な軍事紛争が発生した場合に，海上保安庁または海上保安庁とともに海上警備行動の発令を受けた海上自衛隊の武器使用が警察行動であるならば，戦争ではない。さらに，小規模または限定的かつ直接または間接の武力攻撃や侵略が開始されたときには，日本は独力で対処し，その事態が大規模紛争に発展したときは，日米安全保障条約第 5 条に基づいて米軍の来援を求めることとなる。この段階での紛争は，祖国防衛戦争となる。

自衛隊が保有するすべての兵器を用いて敵を殺傷し，物を破壊することが許されるのは，自衛隊法第 76 条により，総司令官である内閣総理大臣から防衛出動が下令されたときである。防衛出動が下令されると，海上保安庁は自動的に海上自衛隊に編入され，保有する武器を使用して武力行使できる。武力行使には，警察官職務執行法第 7 条の規定である正当防衛，緊急避難，および危害許容要件は適用されず，国権の行使として敵を攻撃し，損害を与えても，器物損壊罪，殺人罪，傷害罪などは一切適用されない。

海上における警備は，第一義的には海上保安庁の任務であるが，海賊対処，領海侵犯の紛争事件，テロリスト行為など，海上保安庁の処理能力を超えた治安の混乱が発生したときには，陸・海・空の 3 自衛隊は，内閣総理大臣の自衛隊法第 82 条の海上警備行動の発令によって警察行動として対応することになる。

海賊対策のための海外派遣も，本来は国際海上警察の任務として海上保安庁の大型巡洋巡視船が担当すべきとされる。日本の海上自衛隊の権限からは，洋上で海賊行為に対応する場合，まずラウドスピーカーで制止し，最終的には海賊船舶と被害船舶との間に艦船が乗り入れて防護することになっており，海上警備行動の発令がない限り，武器の使用は認められていない。一方，海上警察としての海上保安庁の巡視船は，犯罪取締りの警察権が与えられ，海上保安庁法第 20 条に船体射撃が規定されており，極めて厳しい制限の下に武器使用が許されている。

2-3. 朝鮮半島有事の国家危機管理システムの確立

朝鮮半島有事の事態が発生すれば，直ちに約 2 万 8,000 人の在韓邦人と平均 1 日約 3 万人の日本人観光客やビジネスマンなどの滞在者を合わせて，約 6 万人の日本人保護および救出が緊急の課題となる。

朝鮮戦争は終結しておらず，休戦状態であることに留意する必要がある。万一，朝鮮半島で軍事紛争が始まれば，国連軍が機能を開始するため，日本にはその後方支援義務が生じる。国連軍後方司令部は，2007 年にキャンプ座間から移転して，現在横田基地に置かれている。

韓国は，まず自国の防衛，自国民の保護，および在韓米軍家族や非戦闘員などの民間人の保

護に対応しなければならず，６万人の在韓邦人と日本人観光客や業務出張者の保護・救出が優先的に取扱われることはほとんどありえない。日韓の安全保障会議において，韓国は釜山までの陸上輸送は請け負ってくれるが，釜山からの輸送は日本側の任務であるとされる。すなわち，海上自衛隊または海上保安庁に国家行政組織法第２条に基づいて官庁間協力を依頼せざるをえないことになる。

日本の陸上自衛隊による韓国領土内での公務執行が容認される可能性はないため，自衛隊が韓国領土内に上陸して日本人の救出活動を行うことには無理がある。航空自衛隊の輸送機や陸上自衛隊の大型輸送ヘリコプターを受入れてくれない限り，韓国側が最も受入れる可能性のある日本の実力組織は，海上警察であって軍隊ではない海上保安庁となる。したがって，輸送手段としては，釜山港から最寄りの寄港可能な日本の港までを外洋巡視船および民間フェリーによって海上輸送するしか方法はない。結果として，自衛隊が行動できない韓国領土内での在留邦人の集団脱出行動には，沖縄の米国海兵隊の支援が不可欠となる。

なお，このような状況下では，保護しなければならないのは，日本人だけではない。周辺事態法が該当する情勢になれば，日米安全保障条約第６条に基づく後方支援義務として，在韓米国軍人家族約３万人および在韓米国民間人約３万人の日本への避難，さらに，休戦中の国連軍が再結成された場合には，国連軍派遣国の非戦闘員への対応をしなければならない。国連軍には，日本国における国際連合の軍隊の地位に関する協定（地位協定）に関して，米軍と同様に安全保障条約第６条が準用されている。

朝鮮半島有事の際には，ASEAN 諸国，中南米，中近東，および欧州の国連軍に参加した各国からの保護要請が多数もたらされることが予想される。朝鮮半島に隣接するサミット国として，国連軍関係各国の在韓民間人，ASEAN や APEC 諸国の民間人なども，一時的に日本で保護することになる。とりわけ，九州は，避難民を受入れることにより、地方自治体も巻き込む内政・外政問題が発生するため，混乱への対処を想定・検討・考察しておくべきである。

2-4．海賊リスク対策の強化[5)]

ソマリア沖およびアデン湾は，アジアと欧州を結ぶ海上輸送の要衝であるが，この海域ではソマリアの海賊による各国船舶への被害が多発し続けている。最近では，海賊の活動範囲は東方のインド洋にまで拡大し，船舶が最短ルートで航行することが不可能な状態であり，日本の経済･産業にとって大きなリスクとなっている。日本関連船舶の年間通航総数としては，アデン湾で約 2,000 隻，ペルシャ湾で約 3,400 隻が航行しており，原油総輸入量の約 88%を中東に依存し，自動車の輸出台数の約３分の１がソマリア沖・アデン湾からインド洋経由で輸送されているため，原油タンカーおよび自動車専用船などは常に海賊の脅威に曝されている。わが国は，輸出入合計で貿易量の 99%以上を海上輸送に依存し，シーレーンの安全確保は，とりわけ，エネルギー安全保障にとって不可欠な要件である。

現在，ソマリア沖・アデン湾を航行する場合には，追加保険料や警備員の手配などのコスト負担が増大している。なお，海賊を回避するために，南アフリカの喜望峰を迂回すると，６日から 10 日間余分に航海日数を要し，燃料代の増加および納期の遅延を生じることになる。外国人船員の母国では，アデン湾およびインド洋を回避する動きが起きており，日本関連船舶の船員確保が困難となる可能性も生じている。

ソマリアの海賊は，各国の対応に呼応して手法を変化させ，より巧妙かつ凶悪化している。強奪した船舶を母船として活動規模を拡大し，インド洋の東経 70 度付近まで進出しており，船舶を襲撃して数億円の身代金を要求する集団を組織している。捕獲した船員に対しては，母船運航を強要するためや身代金を上積みするために，拷問を用いるなど凶悪化の度合いが増し

ている。

アデン湾は，面積が約 28 万 km^2，長さ約 900km あり，この広大な海域を軍艦船による警備で完全に海賊の活動を抑止することは極めて困難である。日本政府は，2009 年 3 月から自衛隊法により，7 月からは海賊対処法に基づいて，護衛艦 2 隻と哨戒機 P-3C 2 機をアデン湾に派遣している。この活動は，自国だけでなく，他国の船舶も護衛するものであり，海外で高く評価されている。

今後引き続き強化すべき具体的な海賊対策には，以下のような施策が求められている。

① 自衛隊の派遣規模の拡大

護衛艦と哨戒機の増加に加え，護衛艦の活動範囲を拡大するために，補給艦を派遣する。国際協力の観点からは，海賊対処法の改正または新法の制定によって，外国の艦船にも給油可能な態勢を構築する必要がある。

② 自衛隊員および海上保安庁職員による公的警備の強化

海運会社としての船舶の自衛措置と併せて，日本籍船舶に武装した自衛隊員または海上保安庁職員が乗船し，警備の強化を図る。

③ ソマリアおよび近隣諸国への支援

ソマリアでは暫定政府が統治しているが，無政府状態に近く，海賊問題は長期化が懸念されているため，海賊問題の根本的な解決には，国連への拠出の拡充を通じたソマリア暫定政府を立て直すための人道支援がどうしても必要である。さらに，武器輸出三原則の例外化により，イエメンへの巡視船艇の供与を実施することが有効な手段となる。

④国際規則の整備

ソマリアの海賊を逮捕しても，結果的にはソマリアに戻されて，再び海賊行為を働くこととなるのが現状である。したがって，海賊に対する裁判および服役に関する国際的な規則の整備を国連安全保障理事会に働きかける措置を講じる。

3. アセットマネジメント対策とリスクマネジメントシステム 6）

3-1. 社会資本の老朽化の実態と対策

これまでは，日本の高度かつ高密度に整備されたインフラストラクチャー（社会経済基盤）[7] 網によって，高い経済成長と安全・安心で快適な市民生活が実現されてきたが，今このインフラが転換期を迎えつつある。さらに，建築物の耐震化の必要性が強く認識されており，維持・管理の課題として，耐用年数を超えた施設の更新と耐用年数を迎えるまでの適切な予防保全に加え，大規模災害を想定した耐震化にも対応することが求められている。

一方，将来の少子高齢化社会を見据えると，インフラの維持管理に投じられる財源に限りがあり，インフラ維持管理の施策の効率化に加え，さまざまな施策で民間からの資金を投入する必要性が認識される。

地域ごとに社会資本の維持管理を担う地方自治体において，インフラへの投資余力は減少してきており，公共投資分野においても大幅な支出増を期待することは今後難しい。現在，地方自治体が自らの裁量で使用できる財源には限界があり，インフラ更新の必要性を把握していても，そのための資金手当てが困難な状態にある。

財源の面から公共投資に大幅な制約が課されている状況で，迫りくるインフラの大量更新にどのように対応するか，維持管理業務の効率化など新たな処理方法に取組まなければばらない。

社会資本の維持管理・更新の費用は，試算によると，先進的な予防保全を実施した場合でも，投資可能額を上回ることになり，費用の不足は避けられない。したがって，予防保全の徹底がまず実施されねばならない。社会資本を維持管理する実際の業務は，地方自治体が担い，業務に必要な資金調達の多様化およびガイドラインの整備が必要となる。さらに，既存施設の保全が優先されるが，新規建設が必要な場合に

は，国や政令市などが関与して民間の投資を促す事業スキームを構築するような施策も必要になる。

更新が間に合わないことに関しては，老朽化した社会資本を抱える海外でも，インフラに物理的な損傷が発生し，本来の機能提供が困難になる物的クライシスが頻発している。

3-1-1．上下水道管路

全国の上水道資産40兆円のうち高度成長期に整備された多くの上水道施設がこれから更新期を迎える。2020年までに毎年約7,500億円の投資が必要になると試算されているが，実際の費用は試算額以上になる可能性が大きい。しかしながら，地方自治体の水道局事業者のうち財政的に余力のあるところは少なく，職員の不足や高齢化により，必要な更新工事が十分に行われずに先送りされている。耐用年数を迎える水道管路の老朽化は，このままの状態が続けば，社会的に問題が顕在化することが予測される。

水道管路の更新を着実に実施するためには，2つの方策があるとされる。1つは，更新費用の調達方法を多様化することである。現在の起債収入は過去の元利償還に充てられることが多く，必要な建設費に結びつかないため，事業証券化の手法を用い，公的資金以外の資金を調達する方法を取入れることが考えられる。なお，財政が健全な間に将来の更新費用を積み立てる基金を組成する方法を用いることも対象となる。他の方法としては，業務効率化が挙げられる。地元の優れた工事会社や同じ埋設管を扱うガス会社などに施工管理などの上流業務を任せることも有効である。

下水道事業を取り巻く環境は，上水道よりもはるかに厳しいとされる。財政悪化の原因は，下水処理費を適切に回収できていないことにある。すなわち，処理工程で高価な薬剤が多量に必要な高コスト構造にもかかわらず，小規模事業者が多く，経営が非効率であり，料金水準が低く設定されていることが理由である。

このような状況下で，下水道事業者は，民間活力の導入やコスト抑制の取組みを積極的に推進してきた。管路の管理など現場業務の包括委託を始め，今後，より効率的な委託を実施するために，施設の設計から補修までを含めた一体型発注へ委託のレベルを向上させることが必要となる。さらに，下水道事業の収益獲得の機会を拡大させる施策が求められる。これまでも，下水処理の汚泥を有効利用するために，埋設土や緑地，農地の土，および建設資材などへの転用が促進されてきたが，今後は都市鉱山として活用すべく，リンなどの有価物の回収，バイオマスなど再生可能エネルギーとしての利用をはじめ，資源活用を促進する施策が考えられる

3-1-2．橋梁[8)]

道路ネットワークを構成する重要な構造物である道路に設置された橋梁に関して，道路橋で橋長15m以上のものが約15万4,000橋，農道橋で橋長15m以上のものが約3,000橋，林道橋は橋長15m以上のものが約5,000橋存在する。わが国の橋梁は，特に1970年前後に集中的に架設されたものが多く，平均使用年数が50年近くになりつつある。したがって，急速な高齢化の時代を迎え，未点検と高齢化のリスクをかかえていることから，損傷・劣化による事故の可能性が増大している状況にある。

社会資本の維持管理には予防保全が最も有効であるが，全国の市区町村の約4分の1が予防保全に必要な橋梁の点検を実施していないことが判明している。その主な原因は，技術力の不足，予算の確保困難であり，地方財政の逼迫による技術職員と予算の削減が社会資本の維持管理に影響を及ぼしている。

地方自治体の財政力および技術力が低下している状況下で，橋梁を適切に維持管理するためには，民間との連携が不可欠である。具体的には，技術を持つ民間企業や企業連合体が，複数の地方自治体から点検，修繕計画の策定，および工事発注に至る一連の維持管理業務を包括受託するシステムを構築することが最も有効な施策である。

現在の制度からは，橋梁の修繕計画等の行政判断を伴う業務を民間企業が行うことは難しく，発注側と施行側を厳密に区分しなければならないため，実施する上では種々の課題がある。しかしながら，海外では社会資本の維持管理と管理監督業務を一括して民間企業に委託する形態もみられ，わが国でも社会資本の維持管理を民間に開放することは可能である。

3-2. 社会インフラの維持管理と課題

高度成長期以降の大都市部への人口流入に伴い，地方自治体により整備された社会資本の多くが，現在，経済インフラ以上にその維持管理や更新の費用によって自治体の財政を圧迫している。特に，公立学校や給食センターなどが保有・維持する上で最大の問題となっている。

1995 年度施行の地震防災対策特別措置法および 2007 年の生活安心プロジェクトにより，公立の小中学校を早急に耐震化することが決められた。公立の小中学校の耐震化は国全体の問題であり，国は地方自治体に支援をしてきたが，対象施設の数が多いため，維持管理業務の効率化への取組みも進まず，大きな財政負担となっている。

これについては，1 つの自治体で対応するよりも，複数の自治体が共同で建物を更新したり，共同で維持管理を行ったりする仕組みが有効に機能するとされる。自治体にとってだけでなく，業務を請負う民間事業者にとっても，事業規模の拡大やマーケットの活性化につながる利点がある。すでに，公立学校の物品調達では共同調達が進んでおり，公立学校の施設の更新および維持管理業務にもこの仕組みを取入れていくことが必要である。

将来のインフラの維持管理においては，想定される地震などの自然災害への対策を考慮しておかなければならない。東日本大震災では，社会資本の復旧に関する課題も明らかになった。内閣府が発表した東日本大震災によるインフラ関連の被害額は約 16 兆 9,000 億円とされ，このうち道路，河川，港湾などの社会基盤施設の被害額は約 2 兆円で，阪神・淡路大震災とほぼ同程度の規模であった。幹線道路や空港の復旧が早かった理由は，阪神・淡路大震災の教訓により構造物の耐震性が強化されていたことに加え，復旧の優先順位を明確にし，官民の資源を集中的に投入したことによると評価されている。

ただし，民間施設の復旧は，基本的に事業者負担であると定められているため，生活に密着した地方鉄道の復旧は遅れていることが指摘されている。将来，地震災害が発生した場合に，民間が管理する社会資本に対して国がどこまで復旧費用を負担するかについては基準を設ける必要がある。

3-3. 今後のインフラ維持管理リスクの効果的処理手法

これからのインフラの維持管理に関しては，民間活力の導入が不可欠である。世界的にも，利用料の徴収により採算が取れるインフラに対しては，建設から維持管理までを包括的に民間に委託することが一般的であるとされる。改正 PFI 法により，別途法改正が必要な道路と空港を除き，ほぼすべてのインフラに自治体が施設を所有したまま事業運営を民間に委託する枠組みであるコンセッション方式が適用可能となっている。この方式は，公共施設等の運営権を民間に付与することにより，民間企業が自らインフラの利用料金を徴収できるものである。

自治体から事業権を付与された民間企業がインフラの建設・運営を行うコンセッション契約は，利用者からの利用料金で整備して運営コストを賄う方式である。公設インフラの運営を民間企業に委託する方式としては，アフェルマージュ契約という方式がある。一般道路などの一般市民からの利用料収入を期待できないものについては，委託期間が数年以上に及ぶ長期包括委託方式が適用できる。道路の維持管理には，道路の性能基準を定め，その性能発揮に必要な維持管理業務に関し，費用が一定額以下の業務すべてを民間の裁量に任せる契約方式

として，英国ではMAC（Management Agent Contract）と呼ばれる長期包括委託契約が導入されている。今後は，日本でも民間の創意工夫を引き出すために，公共事業の入札などで性能規定型の委託方式が採用できるようにすべきである。

これからは，国や自治体の財政逼迫と人員不足に備え，インフラの整備・維持管理において民間活力の導入を図るために，民間企業にとってインセンティブを持たせることが求められる。今後，公共サービスも可能な限り民間に委託するという考え方に基づき，インフラ整備で民間資金を活用して社会資本整備を行うPFI方式や，維持管理業務の包括委託契約の導入を進めるべきである。民間活力導入のためには，民間事業者の採算性の確保を担保することが不可欠であり，従来の公共事業の発注方式であった単一施設，単一業務を対象とした単純委託の形式から長期間で複数施設，複数業務を対象とした包括委託に変更していく必要がある。過去に整備された膨大で高度なインフラを維持していくためには，従来の枠組みを超えた方法や発想が求められている。

4．サイバーインテリジェンス・リスクマネジメントシステム

4-1．サイバー攻撃の実態[9)]

サイバー空間を通じて国家の治安および外交などを揺るがすスパイ活動であるサイバーインテリジェンスの被害が表面化している。企業の知的財産から軍事機密まで標的は多岐にわたり，サイバー攻撃は安全保障上の重大な脅威という危機意識が国際的に強まってきている。日本の企業や政府機関等へのサイバー攻撃も急増しており，日本が標的の1つとなっていることは確かである。

実際の事例としては，2007年4月に世界初のサイバー戦争といわれる北欧のIT先進国エストニアで発生したサイバー攻撃は，同国の議会，政府機関，銀行，新聞社，テレビ局などのシステムが大規模なコンピューター攻撃を受け，銀行から金銭を引き出せなくなり，決済に支障を来した上に，電気，水道などの一部も機能不全に陥った。単にネット上での被害にとどまらず，甚大な物理的被害をもたらす可能性も増大している。さらに，2008年に，航空機の整備機器がウイルスに感染したために処理速度が低下したことが一因となって，スペインの民間航空機が墜落し，乗客乗員172人が死亡した事件が発生している。2008年6月と10月には，米航空宇宙局（NASA）の地球観測衛星テラの制御システムが2度にわたり計11分以上のサイバー攻撃を受けて乗っ取られた。中国が発信元とされるサイバー攻撃が宇宙空間に及ぶ可能性が明らかにされた。Stuxnet（スタックスネット）と呼ばれる不正プログラムは，これまでのウイルスとは質的に異なり，インフラに直接打撃を与えるサイバー兵器として出現した。実際に，イランのナタンツにあるウラン濃縮核施設のコンピューターを攻撃し，計984台の遠心分離器を誤作動させ，同国のブシェール原子力発電所も一時的に制御不能にした。その結果，核兵器に利用する濃縮ウランを製造できなくなり，イランの核開発を数年遅らせたといわれている。

このように，どの国の政府もサイバー攻撃を受けるリスクを負っている。経済規模が大きい国でサイバー攻撃が発生すれば，被害が一層大きくなり，国家の治安や安全保障を脅かす事態となることが考えられる。金融や電力などの社会システムをコンピューター攻撃で攪乱して経済活動を停滞させ，現実空間でも攻撃を引起すことが可能となっている。複数の手段を併用し，同時多発テロリズムを仕掛けられたら，日本でも国家安全保障を脅かす深刻な事態が発生することになる。企業の場合には，サイバー攻撃の対象となって個人情報が流出すれば，損害賠償や対策のために多額の出費を余儀なくされるだけでなく，企業の社会的評価が低下するなど，

損害は甚大なものとなる。

主なサイバー攻撃の手法は，①サイバーインテリジェンス（三菱重工業，在外公館，および衆議院公務用パソコンの各ウイルス感染にみられるように，ウイルスに感染させるメールを送り付けて，特定のネットワークから情報を盗み出すスパイ行為），②サイバーテロリズム（エストニアで発生した事件のように，正体不明の組織が電力や水道などの公共インフラを機能不全にするなどのテロリズム行為），③ DDoS 攻撃（ソニーグループや官庁サイト攻撃のような，標的とされた企業や政府機関などのコンピューターに対し，一斉に大量のデータを送り付けて機能停止に追い込む手法），などに類別される。

三菱重工業，川崎重工などの防衛産業をはじめとして，衆議院や外務省も深刻なサイバー攻撃を受けたが，問題は，標的型メールによりウイルスに感染して情報が盗み出された可能性よりも，コンピューター内に制御システムを不能にするかまたは誤作動や遠隔操作を引起すウイルスが，密かに埋め込まれる可能性である。

原子力発電施設や交通機関などの重要インフラをサイバー攻撃により稼働停止させることは十分に可能である。たとえば，他国または国際テロリズム組織によって大規模災害の発生時にサイバー攻撃が行われた場合には，甚大な被害が生じる可能性を認識しておくべきである。中国軍はサイバー専門部隊を育成し，すでにサイバー空間での戦闘能力を向上させているとされる。

4-2. サイバー攻撃対策と防御

サイバー攻撃による経済損失は，年間 1 兆ドル（約 78 兆円）にのぼると推定され，国際的にもサイバー攻撃を経済や社会福祉に対する深刻な脅威と認定している。サイバー攻撃は，近い将来に警察の主要な対処領域になると予測されている。サイバー空間での犯罪を取り締る国際法規としては，2001 年に欧州議会が中心となって定め，米国，英国など 32 か国が批准したサイバー犯罪条約がある。同条約については，これまで日本は署名のみであったが，ウイルス作成を含む刑法などが改正されたことによって締結可能となった。したがって，不正アクセスやウイルス作成などの犯罪捜査で連携することが可能となり，犯罪者の引渡しを求めることもできるようになる。

防衛省は，サイバー攻撃に対処するため，2008 年に自衛隊指揮通信システム隊を新設し，省内ネットワークを横断的に監視するサイバー空間防衛隊の稼働を本格化させている。米国防総省は，サイバー空間を陸，海，空，宇宙空間と並ぶ第 5 の作戦領域と位置付けており，専門部隊としてサイバーコマンドを設け，サイバー攻撃に対しては，通常兵器などで対抗するサイバー戦略を発表した。ただし，サイバー攻撃が武力攻撃にあたるかどうかなどについて，国際法上の概念は確立されておらず，国際的な合意もない。外国によるサイバー攻撃と断定された場合に，日本では警察が犯罪として捜査することになり，防衛省が対処できることは限られているとされるが，サイバー攻撃から国土と国民を守るのは，自衛隊の本来任務にあたると考えられる。サイバー犯罪は，捜査自体が容易ではなく，発信源を突き止めようとしても，攻撃者は他人のパソコンを乗っ取ったり，海外のサーバーが経由地として複数使われていたり，途中のサーバーには記録が残らないようにする匿名ソフトが利用され，身元を隠しながら操作をしていることがほとんどで，発信源の特定が極めて困難である。これには，日本の警察の捜査権が及ばない海外を経由していることも大きな障壁となっていることが理由として挙げられる。警察は，三菱重工に対する攻撃をサイバーインテリジェンス，すなわちサイバー空間を通じて国家の治安や外交を揺るがすスパイ行動による被害が表面化した国内初の事例とし，攻撃を国家への脅威と認定した。

サイバー攻撃が，犯罪または国家の安全を脅かす軍事行動のいずれに属するかの判断は，かなり困難なものである。米国防総省は，サイバー

攻撃に対して軍事的に対抗する権利があるとして，通常兵器による反撃も辞さない可能性を示しているが，何が日本への武力攻撃かを規定した武力攻撃事態法でも，サイバー攻撃については明記されていない。急速に攻撃手法が進化する一方で，サイバー空間については，軍備管理条約も存在せず，国際的に対応する制度が追いついていない状況である。

サイバー攻撃の当事者が個人や集団で，狙いがいたずらやデータを盗むことであれば，一般に犯罪行為とみなされる。国際的にはサイバー犯罪条約（2004 年発効）により取り締まりに向けた協力体制ができている。しかしながら，サイバー攻撃の当事者国家で，目的が相手国に重大な被害を及ぼす攻撃である場合には，単なる犯罪の域を超え，国家による武力行使にあたるとされる。ただし，国連憲章や日米安全保障条約など既存の国際法体系においても，サイバー戦争の位置付けは明らかではない。

これまでに未知の領域も多く，明らかにすべき主要な論点は，以下に挙げるようなものが考えられる。

- 公共インフラ機能を停止させることは，軍事的な攻撃にあたるのか。
- サイバー攻撃の出所を突き止め，ネットを通じて反撃することは，応戦になるのか。
- 在日米軍基地へのコンピューター攻撃に日米共同で対処することは，集団的自衛権の行使にあたるのか。

こうした国同士が重要インフラを攻撃しあうなど，脅威の増大を受けて，国家間のサイバー戦争を予防または規制する国際行動規範の策定を目指す動きが欧米諸国の主導で行われている。内容としては，①国家は他国に先制サイバー攻撃を仕掛ける戦争行為を控えること，②一般市民生活に深刻な影響が生じる電力，交通機関，金融機関などの民間システムはサイバー攻撃の対象としないこと，③他国に重大な攻撃を仕掛けた個人やテロリズム組織が自国内にいる場合には，責任をもって取り締ること，などが基本的な草案である。特に，中心となる事項は，従来の戦争で民間施設への攻撃を禁止行為と定めた戦時国際法の考え方をサイバー戦争にも適用することである。

4-3. サイバーセキュリティとリスクマネジメントシステムの構築 [10)]

最近のサイバー攻撃の事件では，IT 技術の発達に伴い，愉快犯などの初歩的サイバー攻撃から進歩して，企業や個人の機密情報を盗み取る攻撃が頻発している。特に，国や政府機関，企業に対する攻撃の手法は，巧妙化，過激化，凶悪化，国際化，高度化，複雑化，多発化，組織化，大規模化している特徴がみられる。とりわけ，明らかに特定の組織を標的とし，主に知的財産をはじめとする機密情報の詐取を目的とした標的型サイバー攻撃が増加している。いかに技術が進歩しても，サイバー攻撃を防ぐ絶対安全・安心なシステムの開発は不可能である。

したがって，下記のように，①特定の組織から情報を搾取して被害を与えることを目的とした標的型サイバー攻撃対策，②重要インフラを含む産業用制御システムへのサイバー攻撃対策，③高度化・複雑化した新たなサイバー攻撃の脅威が顕在化していることを認識して，情報セキュリティ対策を進めるための人材育成を含めた課題に対処すること，が重要となる。

第１に，標的型サイバー攻撃の実態については，従来のサイバー攻撃は，不特定多数のユーザーに不正プログラムを大量配布する方法が多かったが、近年は，特定の組織や個人を確実に感染させることが目的の標的型サイバー攻撃が多く，2007 年から 2011 年の 4 年間で 6 倍に増えている。このような攻撃に対しては，ユーザーが情報を保護するために維持すべき技術基準の策定が必要であり，個々のユーザーがサイバー攻撃を受けた場合に，同様の攻撃による被害を防ぐために，ユーザー，セキュリティ企業，公的機関における情報共有の枠組みとしてのパートナーシップの構築が不可欠である。

第２に，制御システムの安全性確保について

は，現在の制御システムは，外部ネットワークとの接続や制御システムに使用されるOSの共通化が進行しており，サイバー攻撃の脅威が現実化している。これまでのセキュリティ対策は水際対策がほとんどあったため，次のような対策が必要とされる。

・　未然防止対策

　制御システムのセキュリティ基準を作成し，国際標準化を推進する。さらに，国内の制御システムのセキュリティを客観的に評価し，海外に輸出する場合には，海外の認証制度と相互認証に対応できる体制を整備する。加えて，制御システムのサイバーセキュリティテストベッド（セキュリティ検証施設）を整備する。

・　事後対策

　注意喚起情報に関する公開可否の判断規則の検討を含めたインシデント体制の構築を推進する。

・　共通対策

　専門的に優れた人材の育成および安全性確保に対するリスクとコスト意識の醸成を含めたユーザー企業，特に経営者への普及啓発を推進する。

第3に，情報セキュリティ人材の育成が不可欠である。企業のIT基盤をさらに強固なものにするためには，当然ながら，基盤を守る人材が必要となり，特に標的型サイバー攻撃への対応や制御システムの安全性を確保するなどの新たなセキュリティの脅威に対応するためには，新たな技術を持った人材を育成することが必要になる。しかしながら，企業が求める人材と教育機関の教育内容が食い違う状態が生じやすい。

したがって，このような両者の不一致を解消するために，ICT教育推進協議会（ICTEPC: ICT Education Promotion Council of Japan）とNPO日本ネットワークセキュリティ協会(JNSA: Japan Network Security Association）が新たに構築する検討チームによる実践教育に関する詳細な内容の検討，および若年層に対する情報セキュリティ実践教育の場の提供などが必要であることが提案されている。

サイバー攻撃による被害拡大防止のために，重工・重電等の基幹システムで利用される機器の製造業者を中心に情報共有の場を構築する目的から，サイバー情報共有イニシアティブ（J-CSIP： Initiative for Cyber Security Information Sharing Partnership of Japan）が発足した。これは，企業は，サイバー攻撃を受けた場合に，その手口や中身については，公表しづらく，なかなか公表しないため，情報を共有しないと，次の対策が行えないことになり，情報を公開するための規則作りを行ったものである。

具体的な事例としては，(独)情報処理推進機構（IPA： Information-technology Promotion Agency）に，情報セキュリティの専門機関として情報を集約し，秘密保持契約を締結した上で，情報の分析や内容の抽象化を行い，整理して規則を制定し，参加企業間で情報を提供することが考えられている。

電力およびガスなどの重要インフラのセキュリティ強化については，それらのセキュリティ検証施設を構築し，当該セキュリティ検証に関して日米間の協力体制を強化することが実施される。米国エネルギー省所管のアイダホ国立研究所で，重要インフラの制御システムの実機に対して模擬サイバー攻撃を行うセキュリティ検証施設を保有し，研究を行っている。

情報セキュリティ対策に関して重要な点は，コストの問題であり，どれだけ資金を投入すれば安全・安心なセキュリティ対策が確保できるのかが課題となる。セキュリティ分野は，予算上最も削減されやすいが，一旦サイバー攻撃に巻き込まれた事態を想定すると，サイバー攻撃で東日本大震災と同程度の損害事象を被る可能性も生じうることを認識する必要がある。セキュリティをどんなに優れた技術で防備しても，必ず新たなサイバー攻撃手法が出現する。

したがって，100％安全な技術が存在しない以上，常に継続的なセキュリティ対策に取組む以外に方法はないといえる。

5. 資源・エネルギーセキュリティとリスクマネジメントシステム [11)]

5-1. 資源政策の展望

今後，日本にとって，東日本大震災からの復興を進めつつ，持続的成長を可能とするためには，エネルギーを含む資源 [12)] の安定確保が極めて重要な課題である。日本の産業界は，近年の世界的な資源価格高騰により厳しい状況に置かれながらも，高い技術力を背景に資源獲得競争を勝ち抜くために取組んでいる。しかしながら，新興国の経済成長に伴う国際的な需給逼迫や資源ナショナリズムの高揚など，資源を取り巻く環境には極めて不安定な要因が多い。

ここ数年，資源価格は，原油，鉱物資源，食糧をはじめとして急騰している。投機的資金によるマネーゲームの影響もみられるが，中国，インドなど新興国の重化学工業を基盤とする経済成長が加速してきたことにより，資源の需給が逼迫し，価格が押し上げられている現象と考えられる。

濃縮されて経済的な場所に大量に存在するような生産コストが安価な資源または優良な資源は，探し尽くされてしまった。拡大する需要に対して供給不足を解消するためには，濃縮されていない資源や経済的な場所にない資源であっても，確保していかねばならない。その結果，限界生産コストは上昇せざるをえず，資源価格を上昇させる構造的な原因になっている。金融の量的緩和第二弾（QE2）以降，資源市場に投機マネーが入ってきているとしても，背景には世界的な需給の逼迫傾向があるためであり，価格高騰の根本要因は，新興国の工業化による需要の拡大に資源の供給が追いつかないことであるとされる。そこに，海外メジャーによる寡占化という構造問題に加えて，投機マネーの流入が価格高騰を加速させているといえる

多くの資源を海外に依存する日本としては，資源価格の高騰は国の富を資源国に流出させていることになり，産業界にとっては重要な問題として非常な危機感をもってみている。実際に，資源ナショナリズムによって，資源国の一部が輸出規制を始めており，製品の高性能化および高付加価値化に欠かせないレアメタルまたはレアアースの供給が滞るような事態になれば，企業活動に必要な部品や製品の確保ができなくなり，国民生活にも深刻な影響を及ぼすことになる。たとえば，インドネシアでは，自国内で付加価値を高める方策をとるため，自国内での資源加工を誘導する政策を打ち出してきている。このような動きは，日本の産業空洞化につながりかねない。

レアアースを中国が独占していることのリスクについては，尖閣諸島沖中国漁船体当たり事件が発生して，レアアースの輸出が止められる以前から認識されていたことであり，すでに備蓄や調達先の多様化の重要性は指摘されていた。すなわち，中国からのレアアースの供給が停止すれば，高性能な製品，エアコン，洗濯機，ハイブリッド自動車などのハイテク製品が一切製造できなくなるという危機的現状を踏まえ，経済的安定供給と数量的安定供給のためのシステムをどのように構築するか，実効性のある柔軟な対策を検討することは，わが国の脆弱性を強化するうえで必須の課題となっている。

5-2. 資源安定調達の対応策とリスクマネジメント

各国間で資源獲得競争が激化してきているが，国内資源に乏しい日本は，将来にわたり海外資源を安定的に確保し，資源権益の獲得に向けたさまざまな取組みを行っていく必要がある。資源を長期的かつ安定的に確保するためには，企業自ら開発し，権益獲得の努力を継続することが重要である。しかしながら，各国が国をあげて資源獲得を目指している状況においては，民間企業のみの力で海外の資源権益を獲

得することは，容易ではない。資源権益獲得のためには，生産設備、インフラ整備など，巨額の初期投資に加え，調査から生産に至るまでに長い期間を要し，非常に大きなリスクを伴う事業となる。さらに，カントリーリスクおよび低品位鉱床開発が増えることによるリスクも生じる。

このような環境において，日本の資源関連企業は，世界の資源メジャーと規模では比較にならないほど小さく，リスクの受容限度にも大きな格差があるため，日本の企業が対応可能な水準にまでリスクを軽減できるような仕組みが必要となる。したがって，緊密な官民連携システムを構築し，官民一体の投資を行うことが望ましい形態となる。投融資を行う日本企業のリスク軽減策としては，JBIC（Japan Bank for International Cooperation：国際協力銀行），JOGMEC（Japan Oil, Gas and Metals National Corporation：（独）石油天然ガス・金属鉱物資源機構），NEXI（Nippon Export and Investment Insurance：（独）日本貿易保険）など，政府系機関の有する補完機能を拡充することが考えられる。

具体的には，①金属鉱物等の探鉱・開発に必要な資金の供給を目的とするJOGMECについて，原則5年程度とされている出資期間を延長し，長期間にわたる開発を支援する海外投資等損失準備金制度を恒久化すること，②鉱山開発事業者への税制優遇措置を拡充すること，などが政策として必要とされる。

最近の鉱山開発では，多額の建設資金を要する事例が増えており，鉱山だけでなく，道路や港湾などのインフラ整備のコストも膨らんでいる。これまでインフラ整備のコストは開発費用として，ほとんど企業が負担してきた。今後は，資源安定確保のために，JOGMECから鉱山プロジェクト固有のインフラ整備に対し，国策として資金を提供することなどを検討すべきである。とりわけ，政府機関の資源金融制度を有効に活用して資金調達するような官民連携を推進しながら優良鉱山の開発を推し進めることが求められている。

海外資源に依存する状態は，絶えずさまざまなリスクを伴う。日本は，世界第6位の広さを有する領海および排他的経済水域を持ち，そこには海底熱水鉱床やメタンハイドレートなどの鉱物資源が多量に確認されている。国内の資源開発としては，いち早くこれらを利用可能にするための開発に取組んでいかねばならない。しかしながら，この日本近海の海底資源開発は，民間主導では不可能である。政府は2018年度を目途に商業化の実現を目指しているが，技術や予算の制約に加えて，国際的な諸外国との問題が絡んでくるため，外交力を駆使し，国産資源の確保につながる政策の立案と遂行が課題となる。

資源外交について，政府レベルで資源国との関係強化を図ることは，海外資源権益を確保していくうえで非常に重要な戦略である。特に，資源国が開発途上国である場合には，資源開発に伴う環境保全技術，人材育成など多層的な協力に対する日本への期待も大きい。資源獲得競争が激化するなかで，権益交渉が資源国優位の状況にある。日本に対する資源国の要求は，一層厳しくなってきており，これまでのように資金を出しさえすれば権益を買える時代は終わったとされる。将来的な資源政策と長期的な視点に基づき，戦略的な権益交渉を行っていかねばならない。資源国の政治情勢等客観的な状況を適切に捉え，相手国のニーズに応じた多層的かつ多面的な協力を行い，資源国との関係強化を図っていくことが不可欠である。

さらに，国際的で長期的な視点に基づく資源戦略において重要な課題は，人的ネットワーク構築のグローバル化推進である。すなわち，将来，資源国の資源政策に携わるような人材との人的ネットワークを充実させることが挙げられる。国際間の交渉力を駆使する場合に，その橋渡しができる人材を育成するシステムを構築しておくべきである。

さまざまな製品において，高付加価値化，高性能化，または小型化のために，レアアースをはじめとするレアメタルが使用されているため，レアアースなどのレアメタルの確保は，メーカーとして死活問題となり，レアメタル資源を直接調達する場合とそれらを含んだ部品または製品のかたちで調達する場合がある。調達するものに関しては，原料供給国や地域（サプライヤー）を分散することにより，リスク処理が行われる。ただし，部品または製品のかたちで調達する場合，そのなかにどんな原材料がどのくらい含まれているかを把握することは，各部品メーカーの企業秘密とされている場合が多いため，困難である。したがって，全体的な部品調達の供給網（サプライチェーン）のなかで，何がどれだけ必要かを把握し，戦略的に資源を確保するためには，原材料が見えるようにする仕組みが必要とされる。戦略的な資源確保については，希少な原材料の使用量を削減する方策，および代替材料を使用して同等の性能を維持できるような技術開発を推進することが考えられる。

日本の資源確保戦略においては，資源の供給制約が強まる中で，資源外交，省資源技術（使用量低減技術），代替材料の開発，資源のリサイクル技術が，これからも重要なリスク対策となる。そのためには，先端技術産業と資源産業がリスクを共有することが重要である。資源には，生産量の偏在を背景にした資源ナショナリズムによって，人為的に供給不足がつくりだされている現象がみられるが，資源戦略には，直ちに対応すべきことと，長期的な視点から捉えて対応すべきことに分けて取組み，それぞれに応じた対策をとる必要がある。

おわりに

地球的規模で対応が必要となる潜在的巨大災害リスクとしての小惑星衝突リスクおよび感染症リスクの処理に関しては，国際的なリスク対応協力体制を構築することが不可欠である。安全・安心な社会を確保するためには，グローバルな地域・広域連携の醸成やネットワークの形成・構築に基づき，国際的な産官学連携の集大成として，知的財産の管理･活用によるイノベーションの創出が重要である。それによって，他の関連するリスクへの対応システムを整備する基盤を形成することも可能になり，国家の危機管理能力を高めることに繋がると考えられる。

海上の危機管理メカニズム構築に関しては，アジア・太平洋における中国の安全保障上の潜在的脅威が急速に増大し，特に南シナ海や東シナ海での紛争では，先制攻撃により周辺海域を支配する戦略の中国に対応する必要がある。海洋強国を目指して海軍が重視されている背景には，経済成長に伴いシーレーン（海上交通路）確保の意義が増していることに加え，資源確保のため南シナ海や東シナ海での海洋権益を守る重要性が高まっていることが挙げられる。ASEAN 諸国，インド，および米国との政治，経済，および安全保障分野での協力・連携強化が一層必要となっていることを的確に認識すべきである。

社会資本の維持管理に関しては，近年，高度成長期に集中的に整備された社会基盤の老朽化が，全国的に深刻な問題を生じ出している。財源の捻出が厳しい中で，大規模修繕が一時期に集中することを回避するには，従来の対症療法的発想による事故対応型の維持管理から一定期間ごとに検査・点検を実施し，計画的な補修によってアセットの寿命を延ばす予防保全型の維持管理への転換が必要となる。予防保全では，施設・構造物の劣化状態を適切に判断することが重要であり，従来の目視点検から超音波，電磁波，赤外線などの先端技術を利用した点検・検査技術とその評価方法の開発が，今後の災害対応も含めたアセットマネジメントのシステム構築に欠かせない手法として期待されている。

サイバーセキュリティのリスクに関しては，2011 年 4 月に発生したソニーグループの個人

情報漏洩事件や同９月に起きた三菱重工をはじめとする防衛関連メーカーへの情報漏洩事件など，サイバー攻撃事件が多発し，１件あたりの規模も大きくなっており，発生件数は減る見込みがない状況である。このサイバー攻撃に関しても，災害への対応と同様に，その場限りの対応をいろいろな人が勝手にしたり，相手によって異なる対応をしたりせずに，窓口を一本化して処理すべきである。基本的には災害への対応と共通して，問題が発生した場合には，誰が何をすべきか，事前に手順を明確にしておく必要がある。情報を誰に集中させて，どのように対応するかを決め，初動に遅れが生じないようにしなければならい。とりわけ，情報漏洩問題のような危機管理は，時間との勝負であるため，システム復旧等に迅速な対処ができる体制を整備しておくことが前提として必要である。

災害の危機管理におけると同様に，情報としてのインフォメーションは，価値観が伴ったインテリジェンスにしなければ意味がないといえる。災害発生時にはとりわけ，数値情報だけでは役に立たないことが多い。価値観を持った情報であるインテリジェンスが重要となる。その結果，関係者が情報認識の共有を図ることに意味が出てくる。それによって，組織における各自の役割を理解し，実行することが可能となり，効果的なシステムとしての災害対応体制が構築されることに繋がる。

資源・エネルギーの重要性に関しては，石油についても長年指摘されてきた経緯がある。日本経済は，1970 年代の石油危機や 2003 年のイラク戦争など，中東情勢に翻弄され続けてきたが，未だ原油の中東依存からの脱却は進展していない。インドネシアなど中東以外の産油国でも国内消費量が増加し，輸出余力がなくなっているために，日本の原油輸入の中東地域依存度は，2010 年時点で 86.5%と高いままである。ロシアからの原油輸入や天然ガスへの切り替えを推し進めているが，資源開発には，油田開発への資金支援や経済協力をパッケージにした資源外交をもっと積極的に展開すると同時に，資源権益を拡大すべく海底資源開発に取組むことが喫緊の課題である。日本は石油輸入に占めるイランの比率が１割にのぼり，ホルムズ海峡封鎖のシナリオを考えると，日本経済が直面しているリスクへの対応の難しさが認識される。

［注］

1）　Global Risks 2012, Seventh Edition, An Initiative of the Risk Response Network, World Economic Forum, Insight Report.

2）　Chapman, C. R. and D. Morrison: Impacts on the earth by asteroids and comets: assessing the hazard, Nature, 367, 1994, pp. 33-40；藤本浩介，今村文彦「K/T-Impact による津波の発生」『土木学会海岸論文集』第 44 巻，315-319 ページ , 1994；磯部琇三「小惑星衝突がもたらす巨大津波と人類絶滅の可能性」藤縄幸雄編『天災・人災 - 海洋災害の分析と防災対策』生物研究社, 2006 年, 82-106 ページ；特定非営利活動法人日本スペースガード協会（http://wwwspaceguard.or.jp/），国際スペースガード財団（http://spaceguard.rm.iasf.cnr.it/）。

3）　岩崎恵美子監修 / 佐藤元編集『新型インフルエンザ　健康危機管理の理論と実際』東海大学出版会，2008 年 12 月，石井昇・奥寺敬・箱崎幸也編集『災害・健康危機管理ハンドブック』診断と治療社，2007 年 5 月.

4）　佐々淳行『彼らが日本を滅ぼす』幻冬舎，2011 年，佐々淳行「正論　有事の邦人保護は海兵隊が頼り」『産経新聞朝刊』2010 年 7 月 28 日付，麻生幾「海民襲来」『文藝春秋』2011 年 2 月号。

5）　元山登雄「海上輸送の安全・安心の確保を図るために - 海賊対策の強化に向けた提言」『経済 Trend』2011 年 12 月，社団法人日本経済団体連合会，46－47 ページ。

6）　「予防保全型維持管理の導入に向けて」『土木学会誌』Vol. 95, No. 12, 2010 年 12 月，12

- 48 ページ，日本総合研究所「インフラ老朽化時代」① - ⑪，日本経済新聞朝刊，2011 年 11 月 30 日 -12 月 16 日。

7）　経済活動に欠かせない社会基盤として，道路，橋梁，港湾，空港などは，経済インフラストラクチャーと呼び，安全・安心で快適な国民の社会生活を支える病院，公営住宅，公立学校，および文化・スポーツ施設などは，社会インフラストラクチャーという。

8）　依田照彦・高木千太郎共著『橋が危ない - 迫り来る大修繕時代 - 』ぎょうせい，平成 22 年 10 月，土木学会メインテナンス工学連合小委員会編『社会基盤メインテナンス工学』東京大学出版会，2004 年 3 月。

9）　サイバー攻撃を仕掛けるハッカーは，大まかに以下のような分類がなされる。①システムの脆弱性を見つけ出して内部に浸入することにより，高度な技術力を示唆するパイオニアタイプ，②脆弱性を衝く攻撃が誰にでもできるようにする手法の開発者タイプ，③インターネットを通じて特定の主張を実現しようとするネット市民運動家タイプ，④金銭目的で個人情報や産業情報を窃取する犯罪組織タイプ，⑤各国のサイバー戦部隊などの職業人ハッカータイプ。（「サイバーテロ」『WEDGE』2011 年 8 月号，20－28 ページ。）

10）「サイバーセキュリティと経済研究会中間報告」2011 年 8 月，江口純一「特集　情報セキュリティ政策」『時評』2011 年 12 月号，106-111 ページ。

11）「特集　資源政策戦略化の道筋」『経済 Trend』2011 年 10 月，社団法人日本経済団体連合会，8-21 ページ。

12）　資源とは，濃縮されて経済的な場所にある有用な自然物と定義されている。

［参考文献］

U.S. Department of Defense, Department of Defense Strategy for Operation in Cyberspace, July 2011.

Bostrom, N. and Cirkovic, M. M.(eds.), Global Catastrophic Risks, Oxford University Press, 2008.

羽原敬二「第 3 章　リスク・マネジメント」近見雅彦・堀田一吉・江澤雅彦編『保険学』有斐閣，2011 年 5 月，57-87 ページ.

安全保障と防衛力に関する懇談会『安全保障と防衛力に関する懇談会報告－未来への安全保障・防衛力ビジョン－』2004 年 10 月.

対外情報機能強化に関する懇談会『対外情報機能強化に向けて』2005 年 9 月 13 日 .

大森義夫『日本のインテリジェンス機関』文春新書，2005 年.

『防衛研究所ニュース』（“NIDS NEWS”）

防衛研究所（http://www.nids.go.jp）

日経サイエンス編集部編「感染症の脅威」『別冊日経サイエンス』，日経サイエンス社，2008 年 11 月.