IT 障害に関する分野横断的演習の取組み ― 分野を超えた情報共有と連携協力の仕組みづくりに向けて ―

EXERCISES AGAINST INFORMATION-TECHNOLOGY-RELATED TROUBLES THAT INVOLVE MULTIPLE CRITICAL INFRASTRUCTURES

中野 宏幸[1]・大林 厚臣[2]

[1] M.Phil.（Land Economy）MSc.前内閣官房内閣参事官（NISC）(E-mail:Hir.Nakano@mitsui.com)
[2]Ph.D.（Public Policy） 慶應義塾大学大学院経営管理研究科教授 (E-mail:obayashi@kbs.keio.ac.jp)

IT 利用の進展に伴い、重要インフラへの想定脅威のリスク、分野を越えた IT 障害の発生や波及の潜在的リスクの増大が見込まれる。こうした状況を踏まえ、2006 年度に官民での我が国初めての分野横断的な演習として、「研究的演習」と「机上演習」を実施した。この演習は、内閣官房において、重要インフラ 10 分野と、これを所管する 5 省庁などの参加・協力の下に行ったものである。机上演習では、IT 障害に関する具体的なシナリオを設定して実施したが、これらの活動を通じて得られた知見を知的資産として共有し、また、有効活用することにより、情報セキュリティの向上に寄与していきたいと考えている。

キーワード：危機管理、重要インフラ防護、IT 障害、分野横断的演習

1. はじめに

我が国の情報セキュリティ対策は、2005 年 4 月に、内閣官房に情報セキュリティ政策遂行の中核的役割を果たす「情報セキュリティセンター（NISC）、また、同年 5 月には IT 戦略本部の下に「情報セキュリティ政策会議」が設置され、政府横断的な推進体制が整備された。

重要インフラ対策については、2005 年 12 月に、総合的なアクションプランとなる 3 ヵ年の「重要インフラの情報セキュリティ対策に関する行動計画」（以下「行動計画」という）が同政策会議で決定され、官民の緊密な連携の下、1）「安全基準等」の整備、2）情報共有体制の構築、3）分野横断的演習の実施、4）相互依存性解析の実施、という 4 つの柱の施策に取り組んでいる（文献１）。

IT は、産業や社会活動、国民生活に必要不可欠な基盤を提供している。そして IT のポテンシャルは、地理的あるいは空間的な制約の克服を可能としている。他方、そのポテンシャルゆえに、特に重要インフラ分野において IT に起因する障害が発生した場合には、国民生活や社会経済活動に重大な影響を及ぼす可能性がある。

情報通信ネットワークを駆使した情報システムは、物理的な故障箇所やトラブル発生の原因地点の特定が難しい。情報セキュリティ対策を実施してきている重要インフラ分野でも、異常現象の把握や解析を単独で行うには限界があり、分野横断的に情報を集約し、現象把握と対策立案を行うことが重要となってきている。

このため、行動計画では、重要インフラ（行動計画のなかで「情報通信」、「金融」、「航空」、「鉄道」、「電力」、「ガス」、「政府・行政サービス（地方公共団体を含む）」、「医療」、「水道」、「物流」の10分野とされている。）を防護し、安定的なサービス供給に資するため、４つの柱からなる対策を講じていくこととした。この柱の１つである分野横断的演習は、関係主体間での連絡や連携のあり方を検証し、その強化を図っていくために、毎年度、具体的なテーマを設定し実施していくこととしている。

本論文は、官民で連携して行う分野横断的な取組みとしては、我が国で初めてのものとなる「IT 障害に関する重要インフラの分野横断的演習」の実施方法と今後の課題を報告するものである。

行動計画では、IT 障害への脅威を、①不正侵入、データ改竄・破壊、ウィルス攻撃などのサイバー攻撃等の意図的要因、②操作・設定ミス、プログラム上の欠陥などの非意図的要因、③地震、水害、落雷、火災等の災害、など多種多様な対象ととらえている。

さて分野横断的演習は、行動計画を踏まえ、研究的・試行的レベルから、段階的に進めていくことにしており、行動計画の初年度である 2006 年度は、官民での連絡・連携の仕組みづくりの段階であるため、この仕組みづくりと実効性の強化に寄与する知見を提供していくことを目的として実施した。この目的に沿って、年度の上半期に、IT 障害に着目した演習の意義や方法の理解、机上演習における課題設定など主眼とした研究的演習を実施した。

そして、具体的なテーマの下に課題討議を行う「机上演習」を、2007 年 2 月に、研究的演習と相互依存性解析の知見を踏まえて実施した。

本論文では、まず第 2 章において、新たなリスクと認識される IT 障害について、企業のリスクマネジメントにおける同障害への対応の位置づけ及び必要性を明らかにし、第 3 章において、IT 障害のリスクの特徴を具体的に整理した。これらを踏まえ、第 4 章において、IT 障害に関する演習の意義・期待される成果を整理し、第 5 章及び第 6 章において、分野横断的演習の基本設計の考え方をまとめた。第 7 章から第 9 章まで、実際の演習の方法論とアウトプットを述べ、第 10 章において、演習実施を踏まえた今後の方向性を総括した。

2. 企業におけるリスクマネジメント

社会や企業を取り巻くリスクは変化し、多様化している。IT 基盤のセキュリティ問題の面からは、コンピュータ・ウィルスの増加・多様化、重要インフラにおける情報システム障害、ウィニーなどを通じた個人情報の漏洩などの事例が発生し、不正アクセスなどサイバー犯罪の件数なども増加している。

分野を超えて対応が求められるケースも増えている。経済のグローバル化や IT 化の進展で、サプライ・チェーン・マネジメントや企業間の EDI、アウトソーシングなどを背景に連携が進んでおり、ネットワーク型社会の脆弱性が顕在化してきている。

災害や事故等では、近年、新潟県中越地震や台風、集中豪雨、豪雪等の自然災害、通信電源設備のシステム障害等の事故・トラブルが発生しており、これらの中で、大きな IT 障害が発生しているケースもみられる。

技術や社会が変化すれば、それに伴って必要な安全対策も変化する。その結果、専門家でも気づかない間に、新たな対策が必要になっていたり、規制や基準が時代に合わなくなっていたりする可能性がある。対策の遺漏や陳腐化は、専門分野の境界付近や、新しい技術の普及に伴って起こりやすい。それゆえ新しい IT 技術が関与する障害への対策、あるいは分野間の安全対策の連携は、社会のリスクに対する耐性を高めていくうえで重要な要素と考えられる。従って、演習などで課題を発見して、対策を改善したり、安全基準のより適切な運用などに向けた知見を提供していく意義は大きいと考えられる。

企業にあっては、大規模自然災害や事故等が事業継続やディザスター・リカバリー（Disaster Recovery）のあり方を見直す契機となり、「災害や事故などで被害を受けても重要業務が中断せず、中断した場合でも可能な限り短い時間で回復する」という事業継続が、企業と社会との関係から、強く求められる戦略的課題となっている。

その一方で企業には、経営の効率化を進めることが求められる。企業はリスク管理の面では、事故や災害による被害のリスクと、業績の変動といった事業のリスクに、ともに責任を負うことになる。その場合、自社だけが安全対策をとって利益が低くなれば、安全対策のコストと事業リスクがトレードオフの関係になることがありうる。こうした企業の直面する多様な考慮要素は、企業が安全対策の必要性を感じていても、法令等で求められる最低限や、他社の水準を見ながら横並びのレベルにとどまる要因ともなりうる。市場における競争は一般に企業の効率性を高めるが、それが単純なコスト削減競争になってしまうと、安全対策に影響が及んでしまうこともありうる。

しかし企業が供給するインフラの安全のために何が必要かを、最も良く知っているのは企業自身であろう。対策が横並びになりがちな産業では、リーダー的な企業や業界団体がイニシアチブをとって対策を進める方法もありうる。必要な安全対策の模索は、市場競争の中で生まれるものと、分野横断的演習のように企業間の連携や政府のイニシアチブによるものを、ともに活用することで対策の範囲が広がるであろう。

3. リスクの類型と IT リスクの特徴

社会が直面するリスクは数多いが、対策の共通性から、従来型・新型リスク、危機に移行する様態、被害の主原因などの基準で類型化しうる。本節では、筆者が考えるタイプごとの対策の共通性と IT 障害のリスクの特徴を述べる。

3.1. リスクの類型と特徴

第一の分類として、従来型リスクと新型リスクがある。従来から知られているリスクは具体的な対策が立てやすいが、新しいリスクに対しては、知識や経験の不足を補うために想像力を養うような演習をする必要がある。経済活動のグローバル化や技術の変化によって、IT 障害、テロ、新型感染症など、新型のリスクが増えている。

自然災害は、地震や台風などが多い我が国においては、従来型のリスクと認識されている。しかしながら、災害による被災規模等からすれば、1959 年の伊勢湾台風から 1995 年の阪神大震災まで、1000 人以上の犠牲者が出る災害は発生していない。このため、多くの企業人は大災害を経験しておらず、企業内での対策や知識の伝承が途切れているおそれがある。

危機に移行する様態にも類型がある。地震や物理事故などは危機が発生したことが明瞭だが、水害や感染症は

危機への移行が漸進的であり、有事体制への移行を責任者が決定して人々に周知させる必要がある。IT 障害、感染症の初期などは、異常の発生や被害の全体像が分かりにくいので、関係する分野間で速やかに情報が交換されることが重要である。

被害を生む原因でも類型化できる。物理事故、地震、火災など、物理的破壊が被害の主要因になるものは、設備や現場の管理が安全対策の中心になる。地震に強い建物は防火安全性も高いことが多い。それに対して、人的ミスや感染症など、人の不適切な行動が主因になるものは、人の行動の管理や習慣づけが対策の中心になる。また、犯罪、テロ、風評など、意図的な加害行為によるものは、組織や社会の弱いところを選ぶので、物理的な予防は難しく、組織の内部風土や対外イメージの管理が重要な予防策になるだろう。

3.2. IT リスクの特徴

リスク類型で考えると、IT 障害は新型のリスクである。従来型のリスクは、事例が蓄積されているので、対策が分かっていることが多い。しかし新型のリスクは、事例をあまり蓄積できていないので、経験の代わりに想像力をもってノウハウを蓄積する必要がある。また、IT 障害は原因が見えにくいうえに瞬時に広範囲に波及する可能性がある。そのため、情報共有を中心にした分野横断的な対策を行うことが重要となるが、その取組みは緒についたばかりという状況と考えられる。

IT の技術的特徴として、ハードウェアとソフトウェアの分離が挙げられる。ソフトウェアだけを変えて、ハードウェアの機能を変えることができる。そしてソフトウェア（データ）を伝送することで、遠隔地のハードウェアを簡単に操作できる。IT はハードウェア（実物）とソフトウェア（情報）を分離し、情報の操作だけで実体を変化させるという性質をもつ。

この性質ゆえに IT は、一つのトラブルがネットワークを介して多くの障害を引き起こすリスクをもつ。そしてソフトウェアの異常は、ハードウェアの異常と違って、原因が目に見えにくい。システムの自動化や、機能単位ごとのブラックボックス化は、トラブルの可視性を一層低下させる。また、オープン化や汎用化、ネットワーク型オペレーション（オンライン取引、電子ネットワークやサプライ・チェーン）、外部委託業務の多様化、複数プラットフォームの利用などは、障害の原因と波及先を拡散させることになる。しかし IT は、大規模な実物（ハードウェア）の動員をしなくても、情報（ソフトウェア）だけでかなりの演習を行えるという利点がある。

これらにともなって、IT リスクには以下のような特徴があげられる。

1) 被害波及が極めて高速であり、地域や分野を超えて連鎖的かつ広範囲に及ぶ可能性がある。
2) 自然災害と異なり、被害の波及が地理的に連続していないことに加え、業務の様々な局面に様々な IT システムが導入されていることから、一つの脅威の発生による波及先の推定や危険度の認識が困難である場合がある。更には IT システムが高度化・複雑化しており、事案発生の初動段階での原因究明が困難であるとともに、原因を特定するまでの時間が長期化する傾向がある。
3) 攻撃用のアプリケーションがインターネットで公開されていること等により、様々な攻撃が容易かつ秘密裏に行えることに加え、第三者になりすまして攻撃を行うこと等により容易に攻撃者を特定できないようなリスクの少ない攻撃を行うことができる。
4) 自企業内のみならず他企業や他分野への障害波及の可能性が高い一方で、障害発生のメカニズムや分野間等の依存関係に未解明の部分が多い。

4. 演習の意義

IT 障害のような新種のリスクに対しては、何が最適な準備と対応であるかを知るのは容易ではない。むしろ、どのような障害が起こりうるか、どのような状況に対して準備が不足しているかに気づくことで、弱点を一つずつ解決していくことが現実的であろう。

危機管理の想定練習には、大別して二種類のものがあると考えられる。一つは、定められた行動を習熟して身につけることを目的にするもので、これを「訓練」と呼ぶ。もう一つは、参加者が状況に適した行動を選択して実行するもので、このタイプを「演習」と呼称する。

起こりうる障害と適切な対応が分かっているリスクに対しては、訓練は有効である。しかし IT 障害のような未知の部分が多い新種のリスクでは、特定の訓練だけを繰り返すよりも、演習によって従来の対策の弱点に気づくことが重要であろう。シナリオを変えて演習を重ねることで、発見が集積し、安全対策が多面的になり遺漏が少なくなっていく。これは生産活動の改善になぞらえて言えば、安全性の改善ともいえる活動である。

4.1. 期待される成果

演習から期待される重要な成果は、安全対策の課題の洗い出しである。極端な言い方をすれば、課題をどれだけ多く見つけられるかが成果になる。シナリオに沿って順調に対応ができたとすれば、むしろ演習としては深みが足りなかったということもありえる。

また、検討会では有識者から、「情報システムは、ソフトウェアやハードウェア、OS など異なるバージョンが

使用され、また、バージョンアップされて複雑化しているので、日頃から、いざというときにどうするか、手が動くようにしておかないと、立ち往生してしまう」「ある金融機関では、ディザスター・リカバリー・プラン（Disaster Recovery Plan）の周知を図っていたため、同時多発テロのときにも、社員の安否確認や関係者との連絡がスムースにできたという話があり、危機管理の意識を高めるためにも日頃からの演習や訓練が大切である」といった指摘もあった。

そのほか横断的演習の成果として、連携の仕組みづくりが期待される。演習の準備と実施自体が分野を横断した共同作業であるが、そうした共同作業を経験して、顔の見える人的ネットワークを分野間に作っておくことも重要な成果と考えられる。

4.2. 分野間の情報共有の重要性

IT 障害への対応では、分野間の迅速な情報共有が重要である。Fig.1 は分野横断的に障害が波及する IT 障害の例で、横方向に各分野を並べ、縦方向に時間の経過を表している。まず分野 B、次に分野 A で障害が起こり、それらが複合して原因となって、当該分野で障害が発生する。そして当該分野の障害が新たな原因の一部となって、他分野に障害を波及させる様子を表している。

Fig.1 の全体像は、分野間で情報が共有されてはじめて分かるものである。情報共有がなければ、当該分野で得られる情報は Fig.2 に示したものになってしまう。すなわち、いきなり障害が発生して、原因が不明という状況である。分野 A や分野 B から情報が得られれば、原因の推測が可能である。しかし原因が不明だと回復の見込みが立たず、対策は対症療法的になる。障害が拡大するか否か、今後何が起こりそうかの予想が難しい。そして自分野から情報を発信しなければ、障害の波及先の分野もいきなり障害に直面することになる。

分野間の情報共有があれば、状況は Fig.3 のようになる。他分野で起きた障害の情報が共有されると、波及を予測して初動対応を前倒しに行うことが可能になる。すなわち障害を回避したり、回避できなくても障害に対する準備が可能になる。情報共有によって原因が推測できれば、対策は対因療法的になり、回復見込みも立てやすい。そして自分野からの情報発信が豊富で早期ならば、他分野の対応を助けることになる。

演習で検証すべき点は、障害発生後に適切な対応ができるかどうか、その一つの重要な要素として情報共有が適切にできるかどうかということがある。Fig.4 は情報の送り手と受け手の間で情報伝達が行われる過程を模式的に表現している。最初に、送り手から受け手に情報が送られる。情報の内容が受け手にとって十分であれば情報伝達が完了する。しかし情報に不足や不明瞭な点があ

Fig.1 障害連鎖の例

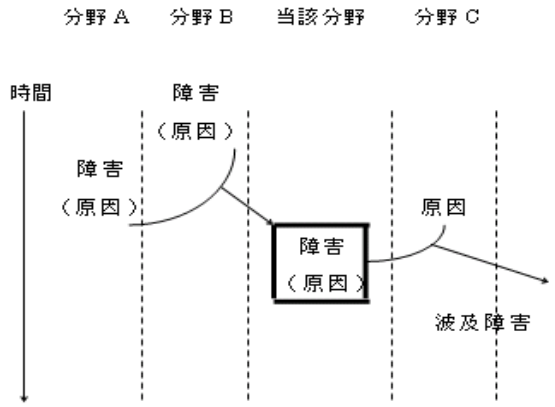


Fig.2 情報共有がない場合

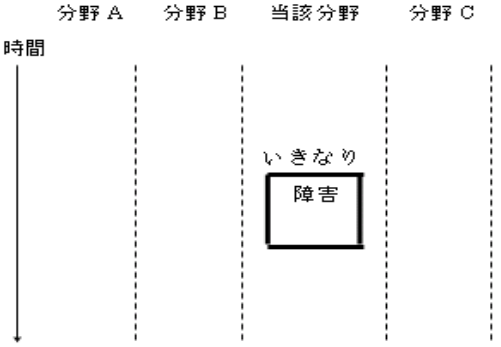


Fig.3 情報共有がある場合

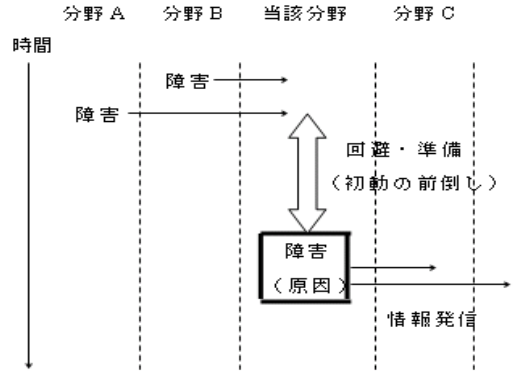
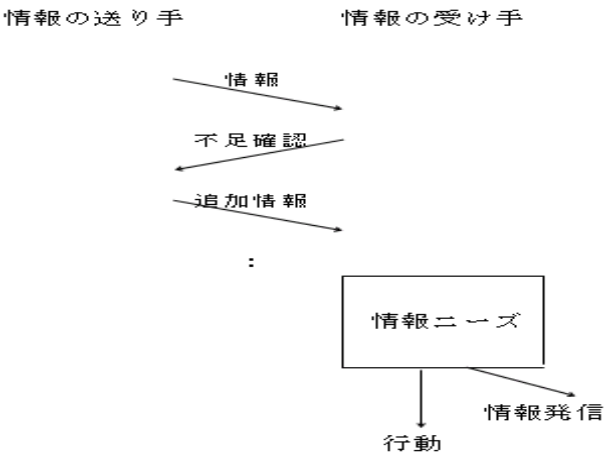


Fig.4 情報伝達の過程



れば、受け手から確認がなされ、送り手がそれに答える。確認は受け手の情報ニーズが満たされるまで、何往復にも及ぶことがある。受け手の情報ニーズとは、受け手の行動や情報発信を支援するものである。情報共有の適切さは、受け手が必要とする内容を、適切なタイミングで、受け手が正しく理解できる表現方法で送られることである。つまり情報の送り手から見ての基準ではなく、受け手の行動が支援されるか否かで判断されるものである。

従来は、IT 障害に関して、分野を超えて情報共有や連携協力するという意識が希薄であった。3.2 節で述べたような IT リスクの特徴から、脅威発生の初期段階における適切な情報の共有が、被害を軽減する上において極めて重要な要素と考えられる。

5. 分野横断的演習の取組み

5.1. 分野横断的演習の背景

重要インフラの安定的なサービス提供は、2005 年４月の第二次提言で述べられているように、「一義的には重要インフラ事業者が責を担うべき」ものであり、そのためには「各重要インフラ事業者がサービスを維持・復旧することが、より容易になるよう各主体が協力することが重要」である（文献２）。そして、分野を超えて、「いつ」「だれと」「どのような」情報連絡や連携を行うか認識を共有し、対応をより効果的なものとしていくかが重要な課題となっている。

このため、行動計画を踏まえ、想定脅威の広がりに対応した具体的脅威シナリオの雛形をもとに、毎年ごとにテーマを設定し、各重要インフラ所管省庁、各重要インフラ事業者、各重要インフラ分野のセプター（IT 障害の未然防止、発生時の被害拡大防止・迅速な復旧及び再発防止の観点から、重要インフラ事業者等のサービスの維持・復旧能力の向上に資するため、重要インフラ分野内での情報共有等を行う仕組み）等の協力を得て、分野横断的演習を実施することとした。

この演習を実施することにより、①重要インフラ事業者における、IT 障害に関する官民の情報共有、連絡・連携のための仕組みの妥当性を模擬的に検証し、緊急時の対応力を強化するとともに、必要な場合は仕組みの見直しにつなげていく、②行動計画の実効性を検証するとともに、高度なスキルを有する人材の育成等、情報セキュリティ基盤の強化に資する、こととしている。

5.2. 国内外の関連演習の実施事例

国内 13 例、海外 26 例の調査によれば、国内については、重要インフラ分野では情報システム障害の分野横断的演習は実施されておらず、防災分野における演習でも、情報システムは稼働していることが前提となっている演習が多いとのことであった。単一の分野での情報システム演習については、電気通信分野におけるサイバー攻撃対応演習（2006 年度）及び電力分野における演習（2005 年度）がある。

欧米では、各国の脅威の認識に対応した演習が行われており、米国では 1990 年代後半から、国家安全保障や国防の観点から、サイバー攻撃を想定した演習が行われている。この中では、サイバー攻撃のみならず、物理的攻撃とサイバー攻撃を組み合わせた演習、自然災害とサイバー攻撃を組み合わせた演習等が実施されている。2006 年２月に実施されたサイバー・ストームには、国内外 150 の機関が参加し、情報共有や組織間連携の確認・検証などを主とする大規模な演習が実施されている。欧米における演習の具体的なシナリオは非公開であり、演習のノウハウなどは専門の演習コンサルタントに集約されており、詳細な状況までは把握できていない。

5.3. 分野横断的演習と相互依存性解析

行動計画にもとづく施策の特徴をとらえると、①相互依存性解析（以下「解析」という）は、各分野にどのような脅威が起こりうるのか、また、それがどのような因果関係で波及するのか、そのメカニズムを解明し、知見を提供していく科学的なアプローチであり、②分野横断的演習は、取組みの実効性や有効性を検証する実証的なプロセスである。

こうした施策の特徴を踏まえ、解析では、重要インフラ間の定性的な関係を把握し、この知見を演習に組み込んで机上演習のシナリオを作り、官民の連絡・連携の枠組みづくりに資することとし、相互にスパイラル的プロセスを担いつつ、全体のレベルアップにつなげていくこととした。国内外において実用化に至っている事例がないことから、試行的な段階からはじめることとした。

解析では、10分野間での定性的な関係の分析の中で、「ITシステムの運用に、通信、電力、水道が重要なリソースである」ことが把握できた。例えば、水道に対する依存意識は一般的には高くないが、阪神淡路大震災では、「空冷式空調機の加湿用水が不足し空調機が停止、結果的にコンピュータが停止した」ことから、「水は重要な対策事項で、今後の重要な課題」と認識されたと報告されている（文献３）。ITに限らず、我々が普段水道に対する依存性を意識せずにすんでいるのは、供給側と需要側の双方で水の供給停止を極力回避する工夫が数多く盛り込まれ、途絶しにくいシステムに十分磨き上げられているからである。

しかしながら、震災等の大規模な災害発生時には、供給側だけでなく需要家側でも水の供給障害が発生する可能性はゼロではなく、水の使用量を把握し、緊急時対応

に備えることは、IT障害発生防止の観点からも必要であることが判明した。

また、個別の分野では見出しえない「分野横断的な取組み」の重要性を認識できたことが、１つの成果であった。即ち、「共助」の重要性への認識が高まった。特に、IT 障害時における情報共有に対する期待が大きいことが明らかになった。

一方、「依存する分野」と「依存される分野」では、認識や取組みに違いがあるものがあり、他分野からどのように期待されているのか、を客観的に把握できた。また、演習シナリオへの知見提供や、ベストプラクティスなど、今後につながる知見を提供することができたと考えている。

6. 2006 年度における演習の基本設計

演習の具体的な検討・設計のため、重要インフラ各分野や所管省庁、有識者から構成される検討会を設置した。有識者には、企業の危機管理、リスクマネジメント、防災、BCP、複数分野のシステムや機能に関する知見、演習のコーディネートなどに関する研究者や専門家が参加した。机上演習の実施を含め、2006 年の 7 月から 2007 年の 3 月にかけて 10 回開催した。それぞれの段階では、ロードマップに示される議論のほか、各段階での議論に資する外部・内部の有識者の説明などを組み込んだ。また、演習と解析の検討会を同日に連続して開催する形式とし、双方の参加者が本委員あるいは他の委員会のオブザーバーとして出席できるようにし、両検討会の意思疎通と参加者の利便に資することとした。

また、情報セキュリティ会議の下に設置されている重要インフラ専門委員会（委員長：浅野正一郎情報・システム研究機構国立情報学研究所教授、委員長代理：土居範久中央大学理工学部教授）には、2006 年 6 月に年度の取組みの方向性、11 月に取組みの中間報告、2007 年の 3 月と 4 月に取組みの総括を報告・審議いただいた。

検討会の進め方については、取組みの初年度として、特に以下の点に留意した。

まずは、年度内で全体の進め方、手段と期待する成果との関係について見取り図をもちつつ、ステップを踏んで進めることとしたということである。具体的には、「Plan-Do-See」と進めていく前に、まずは分野間で連携していく意義、演習の理念や方法について理解を深めていくため、研究的演習の一環として、情報システムの企業実務、防災や危機管理、事業継続計画やリスクマネジメントなどの有識者の講演と議論を行うセミナー形式の検討を行った。これらをベースに、次の「Plan」のステージに入り、今年の演習は、どのような課題設定の下に行うのか、相互依存性解析では何を目指し、どのように進めていくのか、という基本設計の議論を行った。この検討の中では、「そもそも演習や解析は、何の目的で行うのか、目的や成果がみえにくい」という議論もあった。このため、取組みの全体像が鳥瞰できるようにし、「個々の取組みが、マクロの全体像の中で、どのような位置づけにあり、何のためにやっているのか」が一覧できるようにし、目的と成果との関係を見据えつつ、目的意識を明確にしながら、実施した。

そして、「Do」の段階では、具体的にどのように机上演習のシナリオを組み立てていくか、という作業を実施し、「See」の段階で、総括と次のステップに向けての課題を整理した。

さらに、それぞれ分野の特性や事情があるなかでの取組みであることから、１つ１つのステップごとに、各参加者の共通認識や理解が深まるよう、留意をした。

7. 研究的演習

7.1. 演習の概要

「演習は、何のために、どのように行うのか」といった IT 障害に着目した演習の意義や方法の理解、机上演習における課題設定など主眼とし、年度上半期に実施した。演習の手法については、①「何を検証したいのか」「参加者や関係者にどのような意識を醸成したいのか」など、演習の目的や目指す成果について、関係者間で意識を共有することが重要である、②演習を実施し、取組みを検証してみて、次のステップやプロセスに反映できる仕組みとすることが重要である、③演習の規模や準備作業の多寡などを考慮し、継続的な取組みの中では、効果的な演習をどのように行っていくかについて配慮が必要、といった意見があった。

7.2. 他分野からの知見など

演習の実施に当たっては、災害関係で訓練や演習が多く実施されていること、また、IT 障害は災害を含めた物理的障害に伴って発生することが多いことなどを勘案し、災害関係の知見など、他の領域の取組みについて、有識者からの知見を収集した。

他領域の演習からの知見については、①情報連絡や共有の意義、②演習実施の意義、③演習の実施方法や手順、などといった視点から抽出した。

①の点については、以下のような知見が得られた。

1) 災害の事例では、情報が断片的で、情報提供が遅れる、情報が届いても受け手に情報の意味がわからない、現在の情報だけで行動してよいかが判断できず対応に結びつかなかったなど、受け手にとっての十分な判

断材料とならない、あるいは、受け手のニーズと提供情報の間でミスマッチが生じるケースがある。IT 障害についても、障害発生時には、平時の情報共有とは異なる情報伝達が求められる場合があることを含め、IT 障害の特性を踏まえて情報伝達のあり方を検討することが必要。

2) 情報を具体的な対応に結びつけるには、一方的な情報だけでは不十分で、双方向のコミュニケーションが必要。

3) 災害時には、マスメディアなどマクロな情報が発信されるが、一方、企業レベルで意思決定を行うに必要な情報はミクロな情報であることから、マクロとミクロの情報がうまく補完されれば、情報が厚みをまして、迅速かつ的確な意思決定に資する。

障害発生時に、情報共有により原因が推定できれば、次の事態が予測できるし、障害の回避や初動対応の前倒しなどができるので、障害発生からの各段階における行動の判断に資する情報が必要。

②、③については、以下のような知見が得られた。

1) 図上訓練の目的は、地域防災計画や対応マニュアルの習熟とその検証、災害対応の疑似体験と災害イメージの構築、適切な被害把握と状況予測、プロアクティブの原則に基づく意思決定の理解、関係機関との調整課題の理解、計画と実際の運用の乖離の理解など。災害では、疑わしきは行動せよ、最悪事態を想定して行動せよ、空振りは許されるが見逃しは許されない、とのプロアクティブの原則に基づいた行動が重要。

2) 我が国では、自社対応を中心とした障害対策は進んでいるが、外部との連絡・連携を視野に入れた対策は進んでおらず、外部組織との意思疎通や情報連絡の基準を明確にしたうえで、必要な対応を事業継続計画に盛り込んでいくべき。これらも、事業環境や経営方針の変化などに応じた継続的な改定が大切。

3) 演習を効果のあるものとするには、「訓練のための訓練」とならないように留意しつつ、目的の明確化はもとより、継続的な取組みの中でより効果の演習の実施に向けた参加者のインセンティブ醸成、関係者間での情報共有、綿密な準備作業が必要。

4) 行動がフィードバックされる仕組みが重要。即ち、演習を実施し、そのチェックを踏まえてシナリオが改良される、その繰り返しによってシナリオの改良と詳細化が図られる、といった実践が必要。

8. 机上演習

研究的演習を踏まえ、2007 年 2 月に、参加者が一同に会して、IT 障害に関する具体的なシナリオのもとに、会議形式で、課題討議を行う机上演習を実施した。

8.1. 検証課題の設定

官民連絡・連携の仕組みづくり等に資する検証課題を設定し、机上演習の中で課題討議を行った。

8.2. 机上演習の実施に当たっての考慮事項

8.2.1. 理想的な演習のイメージ

理想的な演習は、実体験の代わりとなることが期待される。そのために演習のシナリオは、非日常的な危機の状態を再現し、参加者に心理的な緊張を感じさせながら、リアルタイムに意思決定と行動を迫るものが望ましい。シナリオが現実味を持つためには、実際に起こりうるシナリオである必要があるが、その一方で、平時の想定を超える意外な展開を含むことが望まれる。想定外の状況だからこそ、瞬時の判断が難しくなり、個人と組織の対応能力の限界が試され、対策の弱点が浮かび上がる。

しかし、意外性と現実味を併せ持ち、なおかつ臨場感を与えるような詳細なシナリオを作ることは難しい。そのため一般に危機管理の演習シナリオは、実際に発生した事故の記録をもとに、修正を加えながら作ることが多い。もっとも、IT 障害など新種のリスクは事故の記録が少ない。そして分野横断的なシナリオの場合は、現実味と詳細さを複数の分野にわたって持たせる必要があるため、シナリオ作成はさらに難しいものになる。

シナリオと同様に重要なのは、演習の進行方法である。理想的には、現実に経験するであろう状況と同じ時間的制約の下で、情報収集、情報発信、意思決定、行動が行われることが望ましい。その場合、各参加者の有する情報は、演習開始時には、それぞれが知りうる部分のみとなり、それは参加者ごとに異なることになるが、演習の進行に合わせて、通報や報道による情報など、参加者に追加的に提供されていくことになる。参加者同士が自発的に情報伝達をすれば、それだけ保有する情報が増えていくことになる。

進行係は必要に応じて、参加者に何らかの行動や意思決定、回答を求める。それらの回答や参加者同士のコミュニケーションの内容は、分析のために記録しておくようにする。演習の条件設定によっては、参加者に誤情報や矛盾する情報、不要な情報などを与える、参加者の通信手段を一時不通にするなどの方法もある。演習の会場は、一つの会議室でも良いが、分野ごとに分かれて、分野間の情報交換は電子メールなどの通信手段や相互連絡用のスペースに限るなどの方法もありうる。

想定シナリオにおける意思決定や行動を検証することとは別に、参加者の知見を深めるために、演習終了後に

議論の場をもつと効果がある。議論の時期は、演習直後と後日の両方に行えれば理想的である。演習直後は自分の行動や意思決定の理由を思い出すことが容易である。その一方で、演習から時間をおくと、演習時の行動より優れた対応を思いつくことがある。演習中と違って、冷静に俯瞰的な視点を持てるので、自分たちの集団としての課題や改善提案など､大局的な意見が出ることもある。

8.2.2. 分野横断的演習と組織構造

各分野は複数事業者から構成されており、実際の危機の場面では、行動や意思決定の多くは各事業者によって行われる。同じ分野でも事業者が異なれば、危機における対応は必ずしも同一ではない。そして、各事業者においても、現場レベルと経営レベルでは、持っている情報や権限が異なり、危機対応の役割が異なっている。この机上演習は、分野横断的対応を主眼に置いたものであるが、危機管理に当たっては、事業者間レベルの連絡や、事業者内における経営層と担当者間の連絡なども、もとより視野に入れておく必要がある。

8.2.3. 参加者がもつ情報量の問題

参加者の行動・意思決定の内容は、ある程度まで具体的でなければ「検証」できない。即ち、ある場面での行動を尋ねられて、「最善を尽くす」、「しかるべき報告をする」という回答があっても、実際に適切な対応ができるかどうかは判断できない。従って、回答がそうしたものであれば、司会者は「○○の対応はどうしますか。」などと尋ねることになる。

逆に参加者としては、必要な情報がなければ、具体的な行動や意思決定はできない。演習の状況設定が仮想であれば、参加者は、不完全な情報の下で意思決定を行わなければならなくなるため、シナリオや状況設定は、できるだけ現実に近いものとすることが望まれる。

8.2.4. 初回演習の手法

理想的な演習をあえて表現すれば、8.2.1 節に述べたようなものになるが、今回の演習では、特に以下のようなことに配慮した。

1) 我が国で初めての分野横断的な IT 障害の演習であり、シナリオに参照できるような 10 分野横断的な IT 障害の実例を見出すことが困難であるのみならず、シナリオ作成および演習進行のノウハウの蓄積が少ない。そのため詳細かつ現実味のある分野横断的なシナリオを作ることが難しい。
2) 想定ベースの障害シナリオの場合は、参加者は情報の多くをシナリオから得ることになる。当日にシナリオを知らされても、参加者が状況を把握しきれず、十分に具体的な対応ができないおそれがある。その場合は演習で検証できることが限られる。
3) 大規模な被害を想定して複雑なシナリオとすると、参加者の不慣れや、運営側の進行ノウハウの不足から、演習がスムースに進まず、検証できることが限られる可能性がある。
4) 演習当日の時間は半日に限られている。ただし事前に打ち合わせをしたり、資料を配付したり、当日までの課題を提示することは可能である。

以上のようなことを踏まえ、初回の演習は次のような方法で行うことにした。

1) シナリオの現実味を担保するため、設定の大枠を決めた後に、各分野の方に、シナリオの肉付けや実現可能性の確認などの面で協力いただく。
2) シナリオと各状況に応じた対応に関する質問項目を事前（16 日前）に配布して、どのような行動と情報発信をするか、そのために必要な情報項目は何か、などを演習当日までに各分野内で確認しておいてもらう。また、分野横断的な対応が見込まれる事項を検討しておいてもらう。シナリオの事前開示で、障害の原因と拡大可能性が事前に分かってしまうが、演習ではあらゆる展開を考慮して対応を想定してもらう。
3) 検証の焦点は、初動や分野間の情報共有が適切に行えるか、現時点での分野横断的な課題は何か、などとし、基本的な事項を押さえたシンプルなシナリオとする。負荷の高い状況での情報共有や意思決定の検証等は、次回以降の機能演習の課題とする。
4) 初めての取組みとして、各分野が何らかの形で討議に参加できる全員参加型のシナリオをなるよう、事務局が用意した基本案をベースにして、この趣旨を各分野に伝え、可能な範囲で各分野への波及をシナリオに組み込む。
5) 全参加者を一つの部屋に集めて、ラウンドテーブル形式の机上演習とする。
6) 演習実施後に、演習の感想や分野間・分野内のコミュニケーションのあり方、今後の取組みに期待することなどについてのアンケート表記入を依頼し、事後に回収する。

上記に配慮した効果があって、当日は予定していた質問のほぼ全てを行い、多くの課題の発見があった。演習に続いて行われた討論会では、活発な議論がなされた。

一方でシナリオについては、相当の準備時間と聞き取り調査などを行ったが、10 分野横断のシナリオを作ることは容易ではない。単独分野であってもシナリオ作成は工数がかかるので､今後演習のレベルを上げるにつれて、シナリオ作成はリアルタイム進行のノウハウとともに、演習の成果を左右する要因になるであろう。危機管理の

対策はリスクの種類による差が大きいので、演習はシナリオを変えて数をこなす方が理想的である。そのためにも、質の良いシナリオを効率的に生産する体制を工夫する必要がある。

早期にできるだけ多くの重要インフラ事業者に演習を体験してもらうためには、成熟度の高い共通シナリオを作り上げる必要がある。参加者を変えて同じシナリオを繰り返すと、進行のノウハウも蓄積されやすいと考えられる。共通シナリオにおける各分野の典型的な行動のデータが蓄積できれば、すべての重要インフラ事業者が参加できなくとも、事務局が代行するなどして、演習を実施するような仕組みを作ることも可能である。

しかしながら、「顔の見えるネットワーク」の構築は、障害発生時には何物にも代えがたい貴重な情報共有の基盤になりうる。したがって、重要インフラ事業者が実際に一堂に会して演習を体験し、その内容を議論しあう機会を失うことのないような配慮もきわめて重要である。

8.3. シナリオ選定のプロセス

検証課題を踏まえ、IT 障害の特質を考慮し、シナリオの設定の視点を整理したうえで、想定しうるパターンのなかから、シナリオを選定した。

演習のシナリオのパターンについては、脅威の種別というより発生した障害にどう対応するかに着目し、障害の発生が局所的か同時的か、また、被害波及が限定的か広域的か、などでIT障害の発生を5つにパターン化して、その中から選択することとした。

2006 年度の演習については、1)2006 年度の演習の目的、2)IT 障害の特性、3)官民でのはじめての取組みとして、障害が発生した場合の国民生活や経済社会活動への影響、などを総合的に勘案し、「首都圏の重要 IT 関係施設で IT 障害が発生し、短時間に複数の分野に波及した場合に、どう対応していくか」というシナリオとした。このシナリオは、この演習のために作成したもので、現実の障害として発生することを想定したものではないことを前提とし、事務局で原案を作成し、各分野でチェックをしながら内容を固めていった。

シナリオは次の４つのフェイズからなるものとした。

①物理的な障害が発生する段階

②物理的な障害に起因して、他の分野に IT 障害が発生する段階

③一定の時間の経過後に、IT 障害が他分野に波及し、あるいは想定外の IT 障害が発生する段階

④物理的あるいは IT 障害の復旧の段階

それぞれのフェイズでは、サービス提供側として、現状においてどのような情報発信をし、対応をとっているか質問するとともに、サービスを受ける側として、現状においてとっている対応とサービス提供側に期待する対応をきく設定とした。各分野で有しているニーズと、現状の対応を対比して、分野横断的に認識できるような組み立てとした。

8.4. 演習の実施方法等

机上演習は、重要インフラ 10 分野（情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス、医療、水道、物流）、政府関係者（内閣官房情報セキュリティセンター、重要インフラ所管省庁（金融庁、総務省、厚生労働省、経済産業省、国土交通省））、分野横断的演習関係有識者など、約 90 名が参加し、これら関係者が、一同に会し、課題討議を行う形式で実施した。演習は、2007 年 2 月 7 日午後に実施した。全体を 4 時間の設定とし、前半の 1 時間半をフェイズ①と②、休憩をはさみ、後半の 1 時間半をフェイズ③と④、そして最後の 30 分を各参加者に感想を求める総括の時間にあてた。

机上演習の方法としては、ファシリテーター（進行係）が参加者に各状況に応じた対応に関する質問をし、見解を求める形で進めたが、時間の関係で、事前に用意した質問の順序を変えたり、質問をまとめる、質問を省略する等をそれぞれの時の状況や見解の流れにより、適宜判断しながら進めた。特にフェイズ①と②が論点を多く含み、討議に時間を要するものであったため、前半用に用意した 1 時間半という時間にこだわらず、各分野から示された見解に応じて、「A 分野からは○○という意見があったが、B 分野ではどうか」など、質問をきめ細かにするなどにより、できるだけ多くの分野の参加者に、分野によってスタンスの違いがあるのかどうかを含め、それぞれの事態に応じた見解を示してもらうとともに、内容の確認を行うことに留意した。総じて時間通りに進行したが、最後の総括のために用意した質問事項が多めであったため、各フェイズにもこれらの質問を盛り込み、総括の時間では、演習直後の感想・実感を中心に述べてもらった。

8.5. 机上演習の実施概要

机上演習では、検証課題ごとに以下のような意見があった。

8.5.1. 障害発生時等の分野間及び分野内のコミュニケーションと連携のあり方について

1) 障害発生時の情報共有のあり方については、脅威の早期検知、原因究明の早期化、的確な対応の実施が可能になるよう、障害発生時に、障害の状況や全体像、原因や復旧見通しなどについて、分野を超えて情報を把握できる仕組みを期待する意識が共有されたものと考えられる。即ち、分野によって自分野の対策や復旧に求められる情報や、他分野に提供できる情報が異なり、必ずしも

必要な情報が得られない場合があるので、情報提供や情報共有が有効に機能する体制や仕組みづくりが重要との認識が高まったものと考えられる。

一方、現実的な対応についての配慮が必要との観点から、以下のような意見があった。

① サービス提供側からは、情報発信には努力しているが、障害発生時には、サービスの安定供給の取組みが最優先されるよう努力している。情報発信に当たっては、正確性などが求められるので、両者のバランスが重要である。

② サービスを提供する側は、サービスの安定供給に向けて最善の努力をされている。一元的な情報共有のニーズもある中、どのようなコラボレーションができるか、現実的な対応を考慮し、次のステップのあり方を考えるべきである。

2) また、情報提供の内容やタイミング等については、障害発生時には、可能な範囲で、事実ベースの状況推移を迅速に提供されることが望まれる、との意見があった。

8.5.2. 官民における情報共有・連携のあり方について

官民における情報共有・連携のあり方については、障害に関する情報発信・共有の仕組みの中に官も入れば、共有の幅を広げられるのではないか、IT 障害関係についても、組織体制を含めた効果的な情報共有の仕組みづくりを期待したい、という意見があった。

また、所管省庁や自治体への情報連絡などのあり方については、自治体には、災害や障害発生後、住民からの問い合わせが殺到するので、発生後速やかに、重要インフラ事業者からの情報提供により情報収集するとともに、事業者との連携により住民支援していく仕組みづくりが重要、との意見があった。

8.5.3. IT 障害発生時における迅速な対策等実施のための平時からの対応について

IT 障害発生時における迅速な対策等実施のための平時からの対応については、ハード面、ソフト面での各種の対応が必要との意識を共有しえたものと考えられる。

具体的には、自社のサービスの安定的供給を図るための代替施設の整備などのハード面からの対応に加え、ソフト面でも、緊急体制への速やかな移行と対応など、事象発生時を想定した訓練や体制づくりが重要であるとの意見があった。また、以下のような意見があった。

① システム稼動に必要なリソースについては、例えば、水冷や空調などの水の必要量や備蓄量を再確認しておくことが必要である。

② 緊急時における連絡体制や対応などの運用マニュアル、危機管理プランの整備などが重要である。

③ IT 障害対応のための情報共有体制などを有効に機能させるためには、分野横断的演習など、定期的に共同で、継続して実施することが重要である。

④ 平時から、コミュニケーションを習熟しておくことが大切ではないか。また、効果的事例や教訓、他分野での情報共有事例、過去事例の収集結果などを共有できることを期待したい。

⑤ 障害発生時になって、いつもは使っていない組織や機能を動かそうとしても、うまくはいかないので、平時からも、異常時を意識した仕組みとすべきである。

8.5.4. セプターやセプターカウンシルに期待することについて

セプターやセプターカウンシルについては、分野間で影響があると考えられる情報やその影響度などについて、分野間での情報の集約・共有の場となること、また、日常からのコミュニケーションの場となることを期待したいという意見が多くきかれた。

また、防災との関係については、①大規模災害や IT 障害発生時などにおいて、関係機関からの迅速かつ横断的・総合的な情報を収集できることを期待したい。これらは、的確な復旧対応、被害の最小化に大きく寄与することになるのではないか、②防災などの既存の仕組み・体制の中に、セプターのような IT 障害対応の視点を盛り込んでいくべきではないか、といった意見があった。

情報共有のあり方については、①予防、②リアルタイムでの発信が求められる障害発生時、③被害の拡大防止・復旧、という局面で分けて、対応を考えるべきではないか、という意見があった一方、有事・障害発生時の迅速な対応がセプターでできるのかは、検討を要するのではないか。セプターは、予防などの局面での機能を期待すべきではないか。という意見もあった。

これらに加え、①障害が発生しても、IT 障害に起因するかどうか判明するまでに時間がかかるので、こうした要素も考慮して、共有のあり方を考えるべきではないか、②バックアップ体制の整備などにより、いかなるときでも遅滞なく情報が伝達される仕組みを期待したい、③分野全体で共有すべきものや当事者間だけに限定して検討すべきものがある。セプターにおける情報管理や共有や提供方法について、十分な検討が必要、といった意見があった。

9. 演習の方法論とアウトプット等

9.1. 演習の方法論についての総括

演習の方法論についての総括は、以下のとおりである。

1) 2006 年度の目的に沿った検証課題を設定し、また、ヒアリング調査や事例分析を通じた相互依存性解析

の結果を、演習で実証するという手法により、アウトプットを導出するというアプローチをとった。このアプローチにより、解析と演習をリンクさせつつ、アウトプットを関係者間での意見交換を実施することにより、実証的にアウトプットを導出することができた。

2) 研究的な演習としてセミナー形式からはじめ、共通認識を形成するステップから検討を重ね、年度内でも「Plan-Do-See」のサイクルにより、関係者の理解の増進に寄与しつつ、実施した。
3) 各分野の状況把握などを通じ、個別の分野でのアプローチでは見出しえない「分野横断的に必要な取組み」を発見・整理できた。
4) 障害発生や波及に関する具体的な状況設定、それに対応する質問回答の検討などを通じ、より実践的な検討によるアウトプットが導出できた。
5) 災害などの既存の情報連絡・共有の仕組みとの整合性の確保など、現実的対応に当たっての具体的課題が導出された。
6) 段階的に進めていくアプローチをとり、研究的演習からスタートし、演習のパターンの検討、机上演習のシナリオへの反映・課題討議というステップを通じ、次のステップである機能演習の方法や有効性に関する示唆が得られた。

9.2. 演習から得られた知見と課題

机上演習からは、緊急対応力や障害対応への総合力、平時からの対応力の向上の観点からの知見が得られた。なお、大規模災害などの場合は、物理的な障害と IT 障害が発生することになる。防災については、総合的な防災訓練が行われているが、演習を通じての知見の共有など、関係省庁や機関との連携を強化していくことが重要であると考えている。

これからの取組みを通じ、サプライ・チェーンの進展などの中、関係者間でのリスクに関するコミュニケーションの推進、「自助」のみならず「共助」の考え方の浸透により、社会のリジリエンシーの向上が図られ、国民生活や社会経済活動を支える重要インフラ基盤確立に向けたスパイラル・アップが図られることが期待される。

9.3. 演習を通じた所見

情報共有の意義など、2006 年度の演習を通じた所見は、以下のとおりである。情報共有を通じての分野を超えた連携のあり方、組織における危機管理のあり方、それらによってサービスの安定的供給や事業継続にどのように結びつけていくべきか、といった観点からの意見や所感などが示された。

9.3.1. 情報共有のあり方について

ある分野のサービス停止があった場合、他の分野にどのような影響を与え、どういう対策をとっているのか、また、各分野では、障害発生から復旧までの情報入手や対応をどのようにしているのか、といった分野横断的な対応状況等の体系的理解や、情報連絡の重要性の認識のうえで、有効なものであったと考えられる。

この場合、提供されることが期待される情報は、リソースの復旧予定時刻などの復旧見込み情報であり、当該時刻まで自ら準備している代替能力(自家発電設備の運転可能時間や受水槽等に蓄えられた水の供給可能時間)で十分か、不足する事態が発生するかを判断し、不足する場合は限られた時間とリソースの中で対応策を立案・実行に資する情報が期待されていると考えられる。

また、情報共有のあり方については、以下のような意見があった。

① 情報提供の考え方については、サービスを提供する分野とサービスを利用する分野では、温度差があるように感じられた。情報連絡や共有に関し、効果的なコラボレーションが図られる環境や仕組みづくりが大切ではないか。
② 情報開示の方法などは、リソース供給者とサービス利用者で違いがあったが、ケースが異なれば、どの分野であっても、情報発信の立場にもなりうるという認識を醸成すべきではないか。
③ 依存関係だけに着目するのではなく分野横断的に協力しあえることは何か、という視点が重要ではないか。

9.3.2. サービスの安定的供給や事業継続との関係について

重要インフラサービスの安定的供給や事業継続の視点からは、分野を超えた情報共有の意義は、「いつまでに」「どの程度」「どうする」べきなのか、分野横断的に意識を共有していくことにあり、これを通じて、自分野の今後の方針や目標を更新し、達成目標の実効性を高めていくことができるものと考えられる。即ち、このような演習を通して、自分野の事業継続計画をチェックし、また、それぞれの分野でどのように事前の対策を行うべきかを事業継続の観点から重要度の認識しうるようになる。

また、このような演習を活用することで、事業継続に関する PDCA サイクルを実行し、事業継続マネジメントに結び付けていくことができるものと考えられる。

9.3.3. 演習の意義の理解と組立てについて

演習の場において状況を付与するという演習では一般的にとられる手法ではなく、参加者にシナリオと質問事項を事前に説明し、回答を準備してもらうという方法であったため、演習の場で、「なぜ情報共有をすることが重

要であるのか」を具体的なシナリオに即して実感することは難しい組み立てとなっていた。

また、今回のシナリオでは、物理的な障害を起因とした組み立てで事象の発生が明確であったが、サイバー攻撃や非意図的要因による障害の場合は、当事者以外は、発生事実すら認識できず、知らぬ間に被害を受け、影響範囲が拡大する場合があり、情報共有の重要性を再認識することが重要である。また、障害発生時には、自社に原因があるのか他からの影響かを含め、状況を正確に把握するための情報が必要である。

このため、情報共有の意義が明確になるシナリオ、例えば、「現在発生している事象が自社固有の事情によるものなのか、他の分野に影響を与える可能性のあるものなのか、特別な対応をとる必要があるのか」、「状況付与型演習」とするなどにより必要に応じ、複数の事業者間で、情報交換しながら、原因追及や対応のあり方を検討・判断していくものとすると、相互に情報共有の意義を考えながら、課題も抽出されるのではないかという意見があった。

シナリオの組み立てについては、事務局がトリガーイベントのみを設定し、その後の時間経過によって、演習参加者がシナリオを作成するという手法は、当事者意識を高めるために有効ではないか、といった意見があったが、新たな取組みであるため、さらなる演習討議などでの積み重ねが必要と考えられる。

9.4. 分野の特性の考慮

IT 依存度や IT システムとサービスの安定的供給や事業継続との関係は、分野によって異なっているので、演習実施に当たっても、各分野との関係を考慮して組み立てていくべきとの意見があった。即ち、IT 障害が業務の停止に直結し、IT 障害が主要な経営リスクとなっている分野がある一方、IT 障害より大きな脅威が存在し、その対応にリソースを充てている分野もある。従って、依存度が高い分野での IT 障害の影響や対応を中心に詳細な分析を行うなど、発生する可能性を考慮し、メリハリのある演習や啓発を行うべきとのことであった。

9.5. 企業にとっての危機管理のあり方等について

危機管理のマネジメントのあり方等については、①防災やテロなど、危機管理に対するいろいろな取組みがあって、IT 障害対策につながってくるものもあるので、幅広い対策の中で、IT 障害対策にも配慮していくべき、②IT 障害対応については、システム関係の対応だけでなく、物理的要素や組織や人のマネジメントのあり方も考慮した対応を考えていくべき、③現行の災害計画の中では、IT 関係の扱いは大きくないので、この中に IT 関係も盛り込んでいくべきではないか、といった意見があった。

9.6. 人材育成との関係について

今回の演習では、演習の基本設計、具体的な検証課題の設定、シナリオの策定などを行う演習プランナー、机上演習の進行役を務めるファシリテーターなどの人材の必要性を痛感した。複数分野にわたる実務的知識を持ち合わせた人材に乏しい現状にあるが、分野横断的演習の実施により、これを契機として、ファシリテーターを含め、演習の進め方のノウハウを蓄積し、各分野における IT 障害関係の訓練・演習の実施の企画・運営を行いうる人材の育成が図られることが期待される。

10. 今後の取組みの方向性

2006 年度の取組みは、「それぞれの分野において、何かあったときにどのように対応しているのか」を横断的に把握したうえで、「分野を超えて、連携協力すべきことは何か、共助の取組みとは一体何か」をともに考え、その意義の理解を深めていくというプロセスではなかったかと認識している。分野によって、IT の業務での位置づけ、サービス安定供給との関係などはそれぞれ異なるが、議論を通じて、それぞれ感じ取っていただけたのではないかと考える。

こうした個別の分野や部門を超えてコミュニケーションやコラボレーションによってつくりあげられるもの、いわゆる協調的なポジティブ・サムの要素は、IT 障害に限ったものではないが、漠然とあるような気がしても、実は大変発見しにくいという面がある。その背景には、①個別の利害から一歩距離をおいて、客観的に、分野を超えて大きく鳥瞰してみないとみえてこないという面があること、②こうした発見をする機会がないこと、③ともに考えて発見しようとするインセンティブが働きにくいこと、などがあると考えられる。

このためには、関係の方々とともに考え、コンセンサスをつくりあげていく「場」をもつことが、大切になってくる。IT 障害に対する協調した取組みに向けて、重要インフラ分野の方々に集まっていただき、フェイス・ツー・フェイスで、議論できる機会をもつことができたことは、初年度の取組みとしては大きな意義があったものと考えられる。

2007 年度は、2006 年度の机上演習で発見された知見や課題などを踏まえて、官民の連絡や連携がより円滑かつ効果的に行われるよう、セプターなどを含めて、サイバー攻撃や広域地震など、脅威や障害パターンや状況設定を工夫して、機能向上に向けて、検証課題を設定し、より実践的な演習を実施していくこととしている。

取組みが進んでいる防災の分野でも、重要インフラ関

係の 10 分野が参加して、訓練や演習を行った事例はないと聞く。今回の演習は、IT 障害に関するものであるが、この活動が、今後の分野横断的な取組みのみならず、各分野での活動、また、防災など関連分野での活動にも寄与するものとなることを期待したい。

参考文献

1) 情報セキュリティ政策会議(2005)『重要インフラの情報セキュリティ対策に関する行動計画』 http://www.nisc.go.jp/active/kihon/pdf/bpc01_ts.pdf [2008, March 8].
2) IT 戦略本部情報セキュリティ専門委員会情報セキュリティ基本問題検討委員会(2005)『第二次提言』 http://www.nisc.go.jp/active/infra/pdf/infra_rt.pdf [2008, March 8].
3) ISACA(情報システムコントロール協会)大阪支部(1995)『阪神・淡路大震災の被害分析と危機管理およびコンティンジェンシープランの考え方』.
4) 情報セキュリティ政策会議(2005)『情報セキュリティ基本計画』 http://www.nisc.go.jp/conference/kihon/teigen/pdf/2teigen_hontai.pdf [2008, March 8].
5) IT 戦略本部(2006)『IT 新戦略』http://www.kantei.go.jp/singi/it2/kettei/060119honbun.pdf) [2008, March 8].
6) 佐々淳行(1997)『危機管理』(公務員研修双書)ぎょうせい.
7) Reason, James (1997) 『組織事故』（塩見弘監訳）日科技連(原著 1997 年).

謝辞

分野横断的演習は、各重要インフラ分野の方々、所管省庁や有識者の方々のご協力の下に実施したものであり、あらためて、諸準備や実施に当たってのご協力に感謝を申し上げたい。なお、本稿は、筆者や有識者の個人的な感想、演習から得られた知見を中心にまとめたものであるが、文責は全て筆者にあることを申し添える。

EXERCISES AGAINST INFORMATION-TECHNOLOGY-RELATED TROUBLES THAT INVOLVE MULTIPLE CRITICAL INFRASTRUCTURES

Hiroyuki NAKANO [1] and Atsuomi OBAYASHI [2]

[1] MPhil.(Land Economy), MSc. Former Counsellor of Cabinet Secretariat (National Information Security center), Government of Japan (E-mail:Hir.Nakano@mitsui.com)
[2] Ph.D. (Public Policy) Professor, Keio University, Graduate School of Business Administration (E-mail: obayashi@kbs.keio.ac.jp)

This paper reports activities and findings in the first exercises in Japan against information-technology-related troubles that involve multiple critical infrastructures, which were held in 2006. The activities consisted of research of exercises and on-table exercise, with participation of 10 infrastructure sectors and five government ministries and agencies. The on-table exercise adopted a scenario of event that caused troubles in the information systems and operations of 10 different infrastructure sectors.

Key Words: *Crisis management, critical infrastructure protection, information technology related troubles, exercises.*