1

Research and Development Trends in Critical Infrastructure Protection in the U.S.

AKIHIRO FUJII
Information and Communications Research Unit

1 Introduction

Evaluating the risks that face the infrastructures that comprise our modern society has been given greater emphasis in recent years, particularly from the perspective of homeland security.

The networks that support our everyday lives, such as energy supply (oil and gas pipeline etc.), transportation, communications, and water supply, are in a complex interdependent relationship. Within the context of this interdependent relationship, the information network plays an extremely important role in facilitating the operation of many other infrastructures. At the same time, in order for stable operation of the Internet to be achieved, maintenance is needed from a number of aspects, beginning with information security, but also including the securing of the electricity supply and efficient traffic management.

Research into risk evaluation based on 'interdependency analysis' is extremely important in the context of the security of a broad array of critical infrastructures, and is indeed one of the central issues of research and development aimed at the protection of critical infrastructures. For interdependency analysis, system modeling, computer simulations, and the building of knowledge databases must all be carried out through a highly integrated approach.

In the U.S. today, research projects are being implemented in which, having envisioned the occurrence of an act of terrorism or a natural disaster, interdependency analysis is carried out from multiple perspectives to examine economic impact, and the effect that such an incident would have on public health and on the environment. A total of 14 different defined critical infrastructures, including the electricity supply network, the communication network, the water network, the Internet and waterworks facilities are included in the analysis.

In this report, I will introduce some of the projects being carried out in national laboratories affiliated with the U.S. Department of Energy, where the projects are financed by research and development funds from the U.S. Department of Homeland Security. In particular, I shall focus on research projects concerned with the protection of critical infrastructures based on interdependency analysis, and also aim to give a broader overview of these projects.

2 An overview of science and technology research and development at the Department of Homeland Security

Since the simultaneous terrorist attacks that took place in the U.S. on 11th September 2001, interest in safety and security in terms of homeland security has increased throughout the globe. In the U.S., the Department of Homeland Security Act was passed in November 2002, and in January 2003 the Department of Homeland Security (hereinafter referred to as the DHS) began operations. This department has since played a significant role in homeland security in the U.S. The main pillars of DHS policy are: (i) border security and transportation security; (ii) preparation for and response to emergency situations; (iii) science and technology and; (iv) intelligence analysis and the protection

Table 1 : Main research and development projects promoted by the U.S. Department of Homeland Security

Name of project	Contents	Implementing body
DNDO (Domestic Nuclear Detection Office)	Research on the detection of nuclear substances within the U.S.	DHS, DOD, EPA
CIP (Critical Infrastructure Protection)	Research on the protection of critical infrastructure	DHS, DOD, DOE, NRC
CBTR (Chemical & Biological Threat Reduction)	Research on the response to biological and chemical threats	DHS, DOD, EPA

DHS : Department of Homeland Security
DOD : Department of Defense
DOE : Department of Energy
EPA : Environmental Protection Agency
NRC : Nuclear Regulatory Committee
Prepared by the STFC based on relevant documentation

of infrastructure. In order for these to be implemented practically, the functions of other existing government agencies are utilized.

Within the DHS, science and technology research in the area of homeland security is carried out by the Directorate for Science and Technology, the Directorate for Preparedness, the Office of Intelligence and Analysis, and the Domestic Nuclear Detection Office. Science and technology research can be summarized as 'Defense and Homeland Security (D&HS)', and the three projects as outlined in Table 1 represent the main components of this overall project.

The total amount spent by the DHS on science and technology research and development was 1.5 billion U.S. dollars in 2006, and particularly, the budget of the Directorate for Science and Technology was more than 1.0 billion U.S. dollars. Within the same directorate, the Homeland Security Advanced Research Projects Agency (HSARPA) has been set up, modeled on the Defense Advanced Research Projects Agency (DARPA) within the Department of Defense. A huge variety of research projects are being implemented within the HSARPA.

In this report, I will introduce research trends in 'Critical Infrastructure Protection,' or CIP, within the science and technology research and development being carried out in the field of homeland security in the U.S. I will focus particularly on trends in research that examines risk evaluation based on a method known as 'interdependency analysis.'

3 Implementation structure for projects on Critical Infrastructure Protection (CIP)

CIP is a project that is attempting to construct a computer system that will assist decision-making process undertaken by policymakers by presenting utility functions based on a united evaluation model. Having envisioned a certain disaster, such as an act of terrorism or a natural disaster, this computer system can carry out various simulations on the damage caused to multiple infrastructures and on the subsequent recovery of these infrastructures. In the event that such a disaster actually occurred, various specific questions would emerge: What is the extent of the damage? How much time is needed for recovery? What would the predicted results be for alternative policy choices and alternative responses to the incident? What are the most effective choices for minimizing the damage caused? What are the most dangerous areas, considering the extent and vulnerability of the threat? What investment alternatives / damage mitigation measures / research strategies would be most effective in reducing the overall risk? The CIP system supports the discovery of the most accurate answers to these kinds of questions.

3-1 The implementation structure of the CIP project

Figure 1 shows the positioning of the CIP project within the three projects relating to critical infrastructure protection in the U.S. The CIP project extends across a number of research facilities, including the Los Alamos, Sandia and Argonne National Laboratories, affiliated with the Department of Energy (hereinafter referred to as the DOE). Individual research themes are allocated to these laboratories, and members of each facility cooperate throughout the research.

As can be seen in Figure 1, an organization known as the 'Visualization and Modeling Working Group (VMWG)' exists within the Office

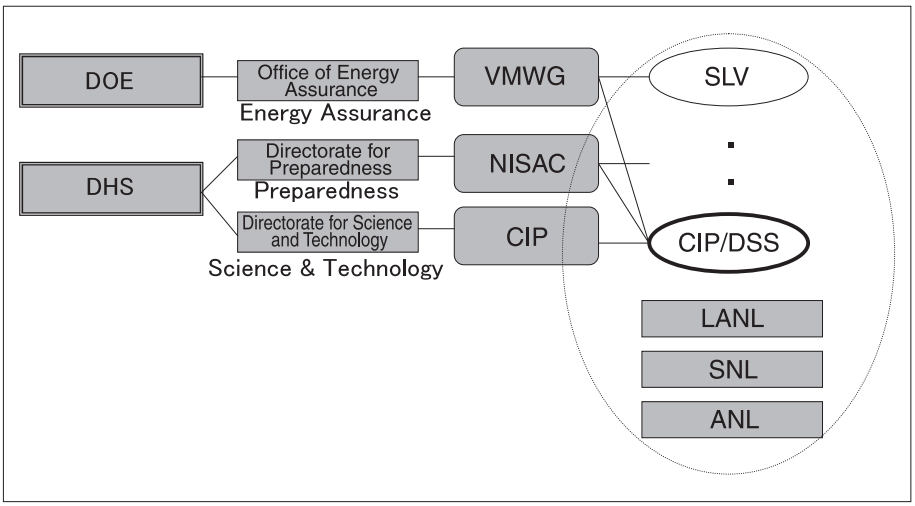


Figure 1 : The three projects on the protection of critical infrastructure in the U.S. and the positioning of the CIP Project within these

VMWG : Visualization & Modeling Working Group
SLV : Scenario Library Visualizer
NISAC : National Infrastructure Simulation & Analysis Center
CIP/DSS : Critical Infrastructure Protection/Decision Support System
LANL : Los Alamos National Lab.
SNL : Sandia National Lab.
ANL : Argonne National Lab. Prepared by the STFC based on relevant documentation

of Energy Assurance in the DOE, and within this organization research is conducted into the visualization of simulation results, known as Simulation Library Visualizer (SLV). At the 'National Infrastructure Simulation and Analysis Center (NISAC)', which is under the jurisdiction of the Directorate for Preparedness in the DHS, researches envisioning various scenarios of terrorism and natural disasters that could affect critical infrastructure are being carried out. This organization is made up of a number of smaller organizations.

The central project in CIP is the Critical Infrastructure Protection Decision Support System (CIP/DSS), which I will describe after the following section. As previously mentioned, this project is concerned with the construction of a system that will aid the decision-making process with regard to various accidents or natural disasters that have the capacity to damage critical infrastructure. Within the CIP/DSS, disaster response research is being carried out, taking into account the 'interdependency' of risks to various infrastructures.

3-2 An overview of U.S. national laboratories - the main implementing bodies of CIP

Within the research and development currently being carried out in the U.S. in area of homeland security (including CIP), the role of national laboratories under the jurisdiction of the DOE is particularly prominent. The DOE operates many of its research programs, including 'nuclear accident response,' the 'chemical, biological, radiological and nuclear (CBRN) countermeasures program,' 'environmental measurement research,' and the 'energy security program,' through these national laboratories, which are under the control of the National Nuclear Security Administration (NNSA).

The three laboratories which I will now briefly introduce - Los Alamos, Sandia and Argonne - play particularly significant roles within this research.

(1) Los Alamos National Laboratory

The Los Alamos National Laboratory (hereinafter referred to as the LANL) is located in New Mexico. It was established in 1943 as part of the Manhattan Project, with the objective of developing the atomic bomb. The most significant role that the LANL has played up until now in science and technology research in the U.S. has been in the context of the development of nuclear weapons. Now, the laboratory conducts technological development with the objectives of establishing the safety and reliability of nuclear weapons, and promoting global security by working towards reducing the threat posed by

weapons of mass destruction.

Like most other national laboratories in the U.S., the LANL is operated under the Government-Owned Contractor-Operated (GOCO) system, whereby the facility is owned by the federal government but operated by a private institution, such as a university. For a long time, the LANL has been operated by the University of California, which played a central role in the Manhattan Project. In 2005, however, an invitation to tender was issued, and since June 2006 the laboratory has been operated by a union made up of several private organizations, including the University of California, the University of New Mexico, and New Mexico State University[4].

(2) Sandia National Laboratories

The Sandia National Laboratories (hereinafter referred to as the SNL) is also located in New Mexico, and was established in 1949. As well as research into 'nuclear weaponry,' the SNL has been engaged in research into 'national defense systems and assessment,' 'energy resources and nuclear nonproliferation,' and 'homeland security and national defense.' In particular, with regard to its work on nuclear nonproliferation, the SNL made important contributions to the safe storage and disposal of nuclear weapons held by the former Soviet Union after the collapse of the communist regime. Amongst these contributions was the creation of employment opportunities for nuclear scientists from that region who could no longer find work at home. The SNL is also operated under the GOCO system. In previous years it was operated by AT&T, but is currently under the operation of Lockheed Martin Corporation.

(3) Argonne National Laboratory

The Argonne National Laboratory is located in Illinois. Like the LANL, it was established in 1946, centered around some researchers who had been involved in the Manhattan Project, which during World War Two had been concerned with promoting the development of the atomic bomb. This laboratory is similarly operated under the GOCO system, and the current operator is the University of Chicago.

4 An overview of CIP projects

4-1 The objectives and research management of the CIP project

The objectives of the CIP project are: (i) calculating the extent of potential damage to those critical infrastructures with certain designated risks; (ii) creating a basic interdependency model for critical infrastructures; (iii) calculating the effect of natural disasters on critical infrastructures; (iv) evaluating the efficacy of damage mitigation measures and; (v) providing practical support measures on region-wide, nation-wide and area-wide scales.

With regard to the research management necessary for the implementation of the CIP project, the following represent the basic thinking behind any such management. First, risks to homeland security must be assessed according to two factors, the 'probability of occurrence,' and 'damage.' It goes without saying that response to those risks which score highly for both factors is important, but in actuality there is a diverse range of issues, with varying levels of risk for both factors.

It is necessary to prescribe each risk clearly from both 'temporal' and 'spatial' aspects. Each phenomenon being examined needs to be classified into either a long-term or short-term risk, and further as either macroscopic or microscopic, and the methods of analysis and response adopted differ according to the nature of these classifications. Within the CIP project, analysis is carried out having selected criteria for the most appropriate perspective, according to the specific nature of the risk.

Further, because this research is concerned with homeland security, attention is also given to the origin of the data or information that will be utilized and to issues of security in terms of the operation of the decision-making support system. The following three standards of judgment are therefore crucial: the 'credibility' of the information upon which analysis will be based, the 'salience' of the information, in other words deciding which information will be given the highest priority, and the 'legitimacy' of the

information, in other words consideration as to whether or not the source of the information handled is trustworthy or not.

In the event of infrastructure being threatened by a terrorist attack or a natural disaster, there would very rarely be a situation in which only a single social infrastructure would be affected. For example, in order to repair damage to energy supply equipment, the transportation network must be used to supply replacement parts to areas where the damage has occurred, and to transport these parts fuel supplies are also needed. Further, the communications network must be functioning normally in order to identify the areas where repairs are needed, and for coordinating any necessary cooperation during the actual repair work on multiple parts of the equipment.

Furthermore, when considering risks to homeland security, it is also necessary to give careful consideration to the trade-off between the cost of risk mitigation strategies, and the benefits that these same strategies create. Amongst the analysis functions of risks that need to be considered are the probability of the incident occurring, the gravity of the effects of such an occurrence, and the cost of protection against any such occurrence, as well as the current status of disaster prevention preparations. Creating a support system for policymakers who have to make judgments on disaster prevention measures means enabling those policymakers to understand the potential effects of disasters more clearly, and thus to take more appropriate and effective measures. In addition, it helps policymakers to make informed choices on strategic disaster prevention investment by identifying any issues likely to hinder recovery.

The main objective of CIP research is to carry out a comprehensive evaluation of risks extending across multiple infrastructures, and to ensure that information that can support the decision-making process in times of disaster is provided to policymakers as quickly as possible.

There are 12 critical infrastructures defined within the CIP Project, as outlined in Table 2. Modeling of these 12 infrastructures is carried out from a two-tiered perspective: the 'national perspective', and the 'designated city perspective'.

Table 2 : Critical infrastructures

1	Agriculture
2	Financial institutions
3	Chemical and hazardous substances
4	Industrial infrastructure
5	Emergency response facilities
6	Energy
7	Food
8	Information and communications networks
9	Post and transit
10	Public health
11	Transportation
12	Waterworks

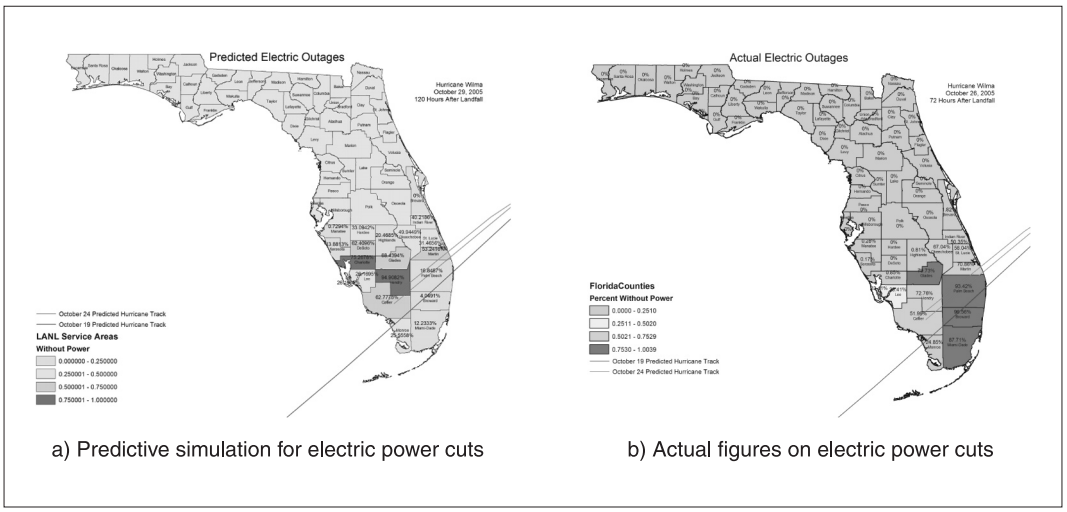
Having set up the model, risk evaluations for individual questions are then analyzed from various perspectives, including 'national defense', 'public health', and 'economic activity'.

4-2 Examples of research results

(1) Real-time damage prediction simulations

Figure 2 shows the results of a recent damage prediction simulation that tracked the path of a moving hurricane, and is an example of the practical application of the results of CIP project research. A simulation of electrical power supply cuts caused by the hurricane was carried out at the Los Alamos National Laboratory, and the results of this have been compared to the actual damage caused. The hurricane in question, Hurricane 'Wilma', was the strongest hurricane ever to be recorded in the U.S., and was first identified on 15th October 2005. It approached Florida from the Atlantic, and dissipated on the 25th. With the hurricane predicted to reach U.S. shores in just a few hours, the LANL received a request for risk analysis, including the likely path of the hurricane. A computer simulation was carried out, and the results of the subsequent risk evaluation were presented to the DHS in real time.

Section (a) in Figure 2 shows the results of the predictive simulation for electrical power cuts on the 19th October, 120 hours after the hurricane was first identified. The probability of electrical power cuts was calculated to be one of four levels for each area: 0-25%, 25-50%, 50-75% and 75-100%. Section (b) in the same



a) Predictive simulation for electric power cuts

b) Actual figures on electric power cuts

Figure 2 : Damage prediction simulation and actual figures for the passage of a hurricane

Prepared by the STFC based on relevant documentation

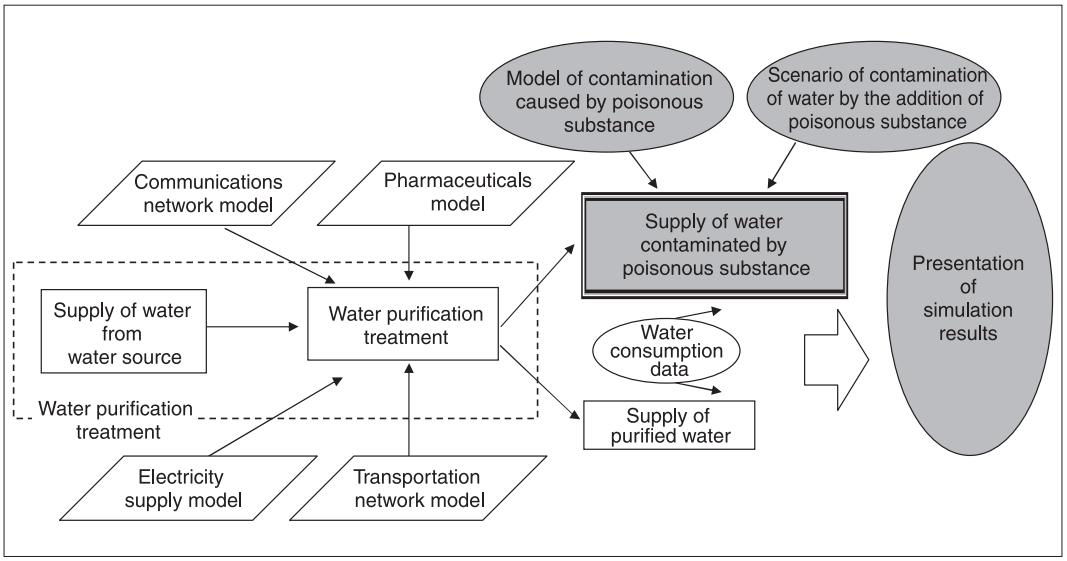


Figure 3 : Analysis case study on the contamination of an urban water system with a poisonous substance

Prepared by the STFC based on relevant documentation

chart shows the actual figures on electrical power cuts for the 26th October for each area. In this example, it can be seen that the results of the advance simulation and the actual damage caused by the subsequent hurricane are in close agreement. As such, this case study clearly demonstrates the high level of the modeling and simulation capabilities of the Los Alamos National Laboratory.

(2) An example of interdependency analysis

Figure 3 shows a flow chart used in predicting damage, based on interdependency analysis, having postulated a scenario in which urban water facilities - a critical infrastructure - have been contaminated by a poisonous substance. Relationships with other infrastructures are outlined, with a focus on water facilities. Actual data on water demand is also referred to, and a number of scenarios are envisioned in terms of the poisonous substance mixing with the water supply. Using the database, which will be referred to in more detail later, a simulation is carried out using a diffusion model, and the level of damage can be calculated using a time series.

In this example, the contamination of water by a poisonous substance has been assumed to have occurred under a number of different scenarios. Here, it is necessary to describe a detailed scenario for multiple potential incidents, and to carry out a quantitative evaluation for each of these incidents. The factors related to

each incident need to be analyzed, the causal and interdependent relationships for each of these factors investigated, and the probability of occurrence for each factor calculated based on the historical record for each. At this stage, interviews with specialists are crucial. Once the probability of occurrence for each factor has been established, a quantitative evaluation of the risks associated with the interdependency of each factor can be carried out by applying, for example, 'Bayesian estimation on the basis of probability theory.' Within this research, the probability of occurrence is shown in models, based on the interdependent relationships of each factor within the scenario.

(3) Other case studies

Within CIP there are also many other examples of research successes leading to the practical application of risk evaluation solutions to a number of other issues. In a case study dealing with the evaluation of the threat of terrorism using bioagents to attack agricultural produce, analyses of the potential effects of various incidents, such as exposure to contagious bioagents, are undertaken, and simulations on the appropriate response to such incidents are also carried out, with details on the production areas and distribution of such cereals as corn, and of domestic livestock such as dairy cattle, beef cattle and poultry having being taken into account.

Another study estimates the extent to which traffic paralysis would occur in the event of various incidents, such as a natural disaster or terrorist attack. Detailed information on population distribution, going as far as specifics on the vocational demographics of individuals, within designated cities is compiled into a database, and the results obtained from the database are used to predict patterns of utilization for the various methods of transport.

An interdisciplinary approach is essential in research such as this. The CIP project is run by a team of researchers with diverse backgrounds. At the same time, the tools used for the simulations necessary for research, such as software etc., are generally existing tools that have been developed for use in other areas.

4-3 Creating a database for decision-making support

The manner in which the results of CIP research are used in problem solving, in terms of the utilization of relevant knowledge, will now be introduced.

First, in order to support the decision-making process undertaken by policymakers in the event of a disaster, a database known as the 'Scenario Library' is available. This is a database of documentation detailing information on previous hurricanes, heat waves, cold weather damage etc., using a standard document format.

The results of modeling and simulations carried out by the CIP team are also stored within this database. These data provide information on the circumstances of the damage caused to the critical infrastructure that was the focus of the research, the modeling technique utilized, the various conditions (priority given to detail, to management time, etc.) necessary for the provision of information to help in the specific decision-making process, the method adopted for practical experimentation, the external visualization method, and the assumed damage to facilities based on either the relevant modeling or simulation.

Within this Scenario Library, the results of risk analysis previously undertaken within the CIP are stored in a uniform digital archive form, and these can thus be used as reference material for any similar analysis undertaken in the future. The operation and utilization of this library is aimed at strengthening the level of knowledge and intelligence on information analysis. When simulating an incident involving bioterrorism, for example, it is possible to analyze and describe the various factors which would comprise the circumstances of such a threat. For example, in the case where an extensive bioterrorism incident is postulated, the question of whether or not there is possibility that a certain bioagent will enter into and contaminate water supply facilities would be one factor in the overall evaluation of the incident. It is also possible to carry out numerical evaluations of situational transitions amongst these partial factors within risk evaluation for facilities that have interdependent relationships.

5 Conclusion

It can be said that the sense of threat that exists in the background to the research introduced in this report is not felt by the U.S. alone, but rather is an issue for all developed countries. Within Japan, also, the need for research and development in the area of risk analysis from a public perspective across a wide range of infrastructures is anticipated to increase. For example, there is concern about the occurrence of a large-scale earthquake in Japan, and the damage from abnormal weather conditions has become more evident in recent years. Compared with the measures being taken by the U.S., Japan' s approach to these issues has fallen significantly behind.

In October 2006, in Honolulu City, Hawaii, the first workshop on the construction of a safe and stable society, based on the U.S.-Japan Science and Technology Agreement was held; discussions were held on the possibility of joint research between the U.S. and Japan on measures to deal with the risks facing extensive areas and social infrastructures, such as terrorist attacks and natural disasters. It can thus be seen that interest in research and development in this field is growing, particularly in the context of international cooperation. However, in Japan, research themes on 'critical infrastructure protection' and 'interdependency analysis,' which were introduced in this report, do not yet benefit from an organized research body structured around a consensus of objectives. Rather, relevant research is spread across a number of ministries and government offices, and under these circumstances it will prove difficult to create a comprehensive research framework for this field.

This report is based on the observational survey that I carried out in 2006, visiting various national laboratories in the U.S. Throughout this survey, I gained the impression that within the CIP research team research was managed in such a way as to facilitate cooperation amongst researchers working in diverse specialized fields, so that common goals could be achieved. In particular, with regard to modeling and the methods used for analysis, it seemed that these were well discussed at each level throughout the organization, and that a common set of basic principles and rules was shared by the whole team. If this field of research is to be promoted within Japan, then I believe that there is a lot to be learnt from the example set by national laboratories in the U.S., with particular reference to the management of organizations.

Within Japan, also, the need for research and development on risk analysis from a public perspective, as well as on preservation and safety, across a wide range of infrastructures is anticipated to increase. We can learn much from the examples of pioneering research and development being carried out in the U.S. For example, there is a need to organize experts from a diverse range of fields, from those specializing in computer-based simulation technology to those involved in the maintenance of specific facilities, within one body. Further, since the results of the research are practically orientated, it is important to examine both the temporal and spatial dimensions of the problem areas, and to then utilize the results of any analysis to aid the decision-making of policymakers.

Acknowledgements

I would like to express my thanks to all of those persons at the DHS, the DOE, the Los Alamos, Sandia and other National Laboratories who so kindly cooperated with my research.

References

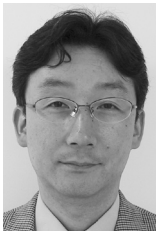
[1] "Strategy to Promote Science and Technology to Contribute to Greater Safety," Council for Science and Technology Policy, 14th June 2006 (Japanese)

[2] http://www.lanl.gov/orgs/chs/biip/cip_dss.shtml, Critical Infrastructure Protection Decision Support System —Department of Homeland Security, Research & Development

[3] National Institute of Science and Technology Policy, "A Corporation has been Selected to be the Management and Operations Contractor for Los Alamos National Laboratory," Science & Technology Trends, February 2006

[4] Mitsuyoshi Urashima, "NBC Terrorism,"

Kadokawa Group Publishing Co., Ltd., February 2002 (Japanese)
[5] Akira Kato, "Terrorism —a Theory of Modern Violence," Chuokoron-shinsha, Inc., May 2002 (Japanese)
[6] Naohide Inoue, "Biological and Chemical Weapons," Chuokoron-shinsha, Inc., December 2003 (Japanese)



Akihiro FUJII, PhD
Information and Communications Research Unit

D. Eng. After being engaged in research on distributed computing and communications protocols, he implemented a project to construct an electronic commerce system. His current area of interest is the impacts that innovations in information and communications technology can have on business administration and national policies.

(Original Japanese version: published in January 2007)