General Explanation
of Special Issue

What Are Dependable IT and Networks?

The information and telecommunications infrastructure of Japan is headed toward a period of dramatic transition as it shifts to an all-IP paradigm, paving the way for the Ubiquitous Society. As a result of the rapid and widespread penetration of the Internet, Japan has already constructed a broadband environment that ranks among the top in the world, and is moving forward with the building of the all-IP Next Generation Network (NGN). Standing at the dawn of the NGN and looking to the future from perspective of the convergence of Information Technology (IT) and IP networks, NEC is focusing on making concrete steps toward the realization of safety and security which are indispensable for public information infrastructures. After first providing a brief explanation of the fundamental philosophy and concepts of the "dependable" IT and networks in this article, we will outline the other technologies to be introduced in this "Special Issue."

General Manager
NEC System Platforms
Research Laboratories
KANOH Toshiyuki

Senior Manager
NEC System Platforms
Research Laboratories
KIKUCHI Yoshihide

Associate Senior
Vice President
NEC Communication
Systems, Ltd.
ARUTAKI Akira

1 Introduction

The widespread adoption of personal computers (PC), mobile telephones and other terminals combined with the penetration of the Internet and other communications networks have given us the ability to enjoy the efficiency and convenience of life in an Information Society. However, there is much room for debate on whether or not everyone feels that a world founded on these information and communication technologies is both “safe” and “secure.” In fact, there are probably quite a few who feel a touch of anxiety or vague doubts about the prospects.

In this article, we will first examine the risks and weaknesses that our present-day Information Society is confronting, and then will discuss the necessity of technologies that resolve the risks/weaknesses. Finally a variety of information and network technologies in this special issue will be abstracted, which NEC proposes for the construction of safe and secure NGN.

2 The Necessity of Dependability

2.1 Concrete Examples

In the highly advanced information society in which we currently live, we are faced with the danger that the damage from one unfavorable incident can rapidly spread and impact a broad area via information and communications networks. The computer virus is a typical example of just such an event, but information leakage through problems with the system itself or unauthorized access, and other cases also have been reported and publicized in the news.

For example, the giant regional blackout that hit North America in 2003 was triggered by the complex combination of various elements including a malfunction in the computer managing the power grid, human error and a local power blackout caused by a fallen tree. In a chain reaction, the blackout spread over a wide region extending from the northeastern part of the USA all the way into Canada. In total about 50 million people in the USA and Canada were affected by the power outage, and the economic toll was estimated to reach billions of dollars.[1, 2] Moreover, too numerous to mention are the frequent occurrence of information leaks, chaos in the stock markets caused by order errors and other incidents that could be called the pitfalls of our ever advancing Information Society.

The bar chart in **Fig. 1** shows the computer/network-related crime statistics by category (CSI/FBI 2005[3]) in North America. The top three crimes in terms of estimated losses as a consequence were computer viruses, unauthorized access and theft of proprietary info. According to the report, the losses resulting from all categories totaled $130 million. These statistics were

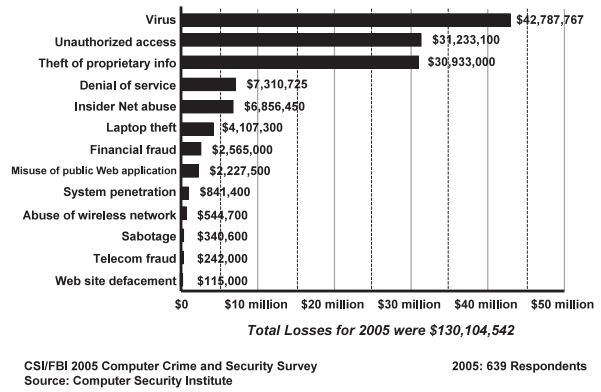


Fig. 1 Losses from computer/network-related crime by category in North America.

based on responses from only the 639 companies that participated in the survey conducted by CSI; therefore, from the perspective of computer/network-related crime throughout the USA or the world, it is clear that the numbers below represent only the tip of the iceberg. **Table** presents data on the extent and scale of damages resulting from unauthorized disclosure of private information in Japan. As some of damages in the Table reach billions of yen, it is clear that information leaks pose a large and growing risk in corporate activities. The safe and secure management of information that is stored in databases in compliance with the Law concerning the Protection of Personal Information enacted last year in Japan has become one of the most important missions of both the public and private sectors. Moreover, terminals that are "always connected" to the Internet are recently suffering an epidemic of malware such as viruses carried by file exchange software that trigger information leaks and viruses that make information stored on PCs visible to unauthorized parties via the web.

2.2 IT and Internet Technology at the Turning Point

It has been conventionally thought that the Internet's characters of distribution and robustness make it particularly suited as a network infrastructure to support information exchange in disaster management and recovery. This relies much on the be-

(Extracted from articles by various newspaper publishers)

	City "A" (regional municipality)	Company "B" (service industry)	Company "C" (retail industry)	Company "D" (financial service industry)	Company "E" (retail industry)	Company "F" (telecom industry)	Company "G" (logistics industry)	Company "H" (service industry)
Date of Incident/Discovery	May 1999	May 2002	June 2003	August 2003	November 2003	January 2004	March 2004	January 2005
No. of Persons Affected	210,000	37,000	560,000	79,000	180,000	4,510,000	132,000	122,000
Disclosed Content	Name, address, sex, DOB	Name, address, mail address, occupation, body size, content of consulting, etc.	Name, address, sex, DOB, telephone no., etc.	Name, address, sex, DOB, telephone no., occupation, annual income, etc.	Name, address, mail address, etc.	Name, address, telephone no., mail address, etc.	Name, address, etc.	Name, address, telephone no., annual kindergarten admission certificate no. and validity period, etc.
Channel of Leak	Unauthorized removal of data from premises by outsource development personnel	Storage of data files in the web server where they were accessible/ viewable from outside the company.	Leaked from the computer of the outsource developer.	Leaked from the computer of the outsource developer.	Leak originating from an outsourced mail server	Unauthorized removal of content from premises by internal personnel	Leaked from the computer of the outsource developer.	Unauthorized removal of content by an employee of the outsourced system administration service supplier
Estimated Loss(*)	(**)	(15 million yen)	280 million yen	80 million yen	180 million yen	2,300 million yen	660 million yen	60 million yen
Remarks	Civil suit seeking damages (Settlement in 7/2002, 3 plaintiffs) Per plaintiff - Compensation: ¥10,000, Legal fee: ¥5,000	Civil suit seeking damages (Currently disputed, 14 plaintiffs) Per plaintiff - Compensation: ¥1.15 million	Distribution of cash coupon (¥500) (Per plaintiff)	Distribution of cash coupon (¥500) (Per plaintiff)	Distribution of cash coupon (¥1,000) (Per plaintiff)	Distribution of cash coupon (¥500) (Per plaintiff)	Distribution of amusement park ticket (¥5,000)	Distribution of cash coupon (¥500) (Per plaintiff)

* Does not include costs related to issuing a public apology (ad placement costs), cost of measures to correct the security problem, damage to corporate reputation (goodwill) from loss of trust, losses arising from self-imposed restrictions on business, etc. ** Associated legal costs up to the Supreme Court and compensation payment.

Table Examples of major leaks of personal information in Japan.

lief that its mesh configuration of transport scheme and the distributed allocation of devices such as routers and servers allow the autonomous re-routing of communications around localized damage in the event of a disaster, thus avoiding paralysis of the entire network.

However, it would not be a mistake to daringly say that the weakness of the Information Society as previously described is something that has been potentially part of the Internet since its inception.

The Internet is characterized as...

- a flat, "open" autonomous distributed system,
- communication that is in principle connectionless and "best effort,"
- and the capability of terminals to execute sophisticated network functions.

With these characteristics as its driving force, the Internet has experienced explosive growth on a global scale. In its infancy, the attraction of its convenience and excellent cost performance (C/P) fueled its popularity as a tool for researches, hobbies and entertainment as well as for the sales promotion activities of companies. Today as a result of its utilization by so many people from all walks of life, the Internet has become the incubator for the birth of a variety of new businesses, and grown into a vital information infrastructure that supports corporate activities and government services.

If we compare the Internet with the conventional information infrastructure of the fixed telephone network, the differences become quite apparent.

The telephone network system is characterized as...

- a system of switches and communication channels in a layered structure,
- communication that is in principle connection-oriented with an assured level of bandwidth,
- and management by an intelligent network separate from the voice transmission channels.

Also in many countries, fixed telephone network systems were deployed as a national project and undergone upgrades and improvements over their history in order to fulfill their vital mission of providing universal service to the citizenry. In America, Europe, Japan and other advanced telecommunications nations where the construction and improvement of the fixed telephone network systems has continued unbated, these systems have reached a point of almost perfect shape and continue to earn the enormous trust of millions of users.

In contrast to the flat, open characteristics of the Internet, the fixed telephone network system is stratified; accordingly, it can be clearly more defensive to malicious attacks on the terminal, network functions and other aspects of the system. However, in response to the needs of users who want the freedom to manage and exchange diverse digital information, it can be said that network resources are limited to a telephony service, because they are mainly devoted to voice traffic.

Serving as a universal service in the future, the Internet is expected to function as an information infrastructure to support the physical infrastructure of electric power, gas, water, traffic and transportation. In order to fulfill this role, it is necessary to achieve safe IP networks in which people can place their full trust and use with total confidence.[4)]

By introducing and incorporating the approach of "dependability" in IT and networks, it becomes possible to overcome a variety of technical problems. At NEC, we believe that the essence of "dependability" is "ideally no occurrence of faults or obstacles at all, but it also encompasses the ability to immediately grasp the situation when some abnormality appears and even predict such events in advance, and to maintain a situation of security without an event leading to social panic or development of catastrophic failure, and to do it at all at a reasonable cost."

3 Technology That Complements Both Convenience and Safety/Security

From the perspective the keywords "convenience" and "safety/security," **Fig. 2** categorizes the needs[6)] related to the ubiquitous networks that will inter-relate and fuse IT and IP networks. By examining this chart, it is possible to grasp expectations for the provision of enhanced convenience but premised on a certainty of safety and security. **Fig. 3** shows a model for technologically addressing these needs that appear at first glance to be inconsistent if not opposed. Three prerequisites for convenience have been identified and listed in the diagram including service addition/expandability and business interface/interlinking with various industries. As for the prerequisites for safety/security, it lists stable operation, automatic recovery (self-healing), and assurance of emergency communications. As for prerequisites that overlap the demands for convenience and safety/security, the diagram shows items such as diversity of ubiquitous terminals and optimal quality.

From these prerequisites, we can see the functions that are demanded to realize services high in convenience and those that will make possible the safety and security of IT and networks as a lifeline. As a result of these finding, the technological model for the next-generation ICT has been outlined in Fig. 3. Though categorized into terminal-, network- and server-related functions, it should be understood that these are not independent but are mutually interrelated. Take for example the "self defense" technology listed in the terminal-related function column. Working in coordination with the network and server functions, this technology prevents information leaks caused by misuse/abuse, attacks on or malfunctions of terminals that store a vari-

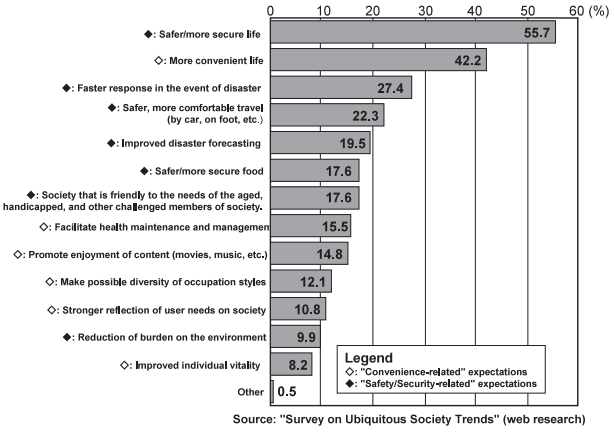


Fig. 2 Growing need for Ubiquitous Networks.

ety of personal information and possess advanced functions, and protects networks from disruption.

4 Dependable IT and Network Technology

The technologies that will realize dependable IT and networks and are introduced in this feature consist mainly those that are currently headed toward commercialization, and those that are currently the subject of R&D with expectations to be realized in the near future.

(1) Network Platform Technology Domain (6 papers)

[A] In the area of security engine technologies that provide a safe and secure environment and their application, this feature introduces the hardware-based security engine, abnormal traffic detection system, and a mail damage avoidance system. [B] Traffic recognition technologies are important for realizing dependable VoIP. An explanation of the IP-network-based traffic identification (discrimination) technologies that serve as the infrastructure for VoIP and supports high-reliability telephone service is provided. [C] Among the system platform technologies that support dependability, we focus on achievement of "open component"-based high reliability and availability management, and introduce the advanced characteristics of the Generation-Free-Platform that incorporates a redundant configuration that transcends the cabinet and an automated redundancy configuration all made possible by optical inter-connection technologies. [D] In the fourth subcategory of network traceability technology that identifies points of declining performance and problem spots in large-scale networks, we look at large-scale, wide-area quality monitoring and trace technology to identify points of performance degradation. [E] In the area of next-generation mobile communications technologies to improve dependability, we examine those that raise the reliability of the next-generation mobile communications system - currently advancing toward standardization, wireless LAN quality assurance technology, and multi-homing technology that utilizes WiMAX/WiFi. [F] Regarding next-generation network security solutions, we explain about mutual complementary defense technology in carrier networks which are continuing to grow in both scale and complexity, behavior-surveillance Intrusion Prevention System (IPS), and carrier network quarantine technology as well as 4 solutions for defense against network attacks, disas-

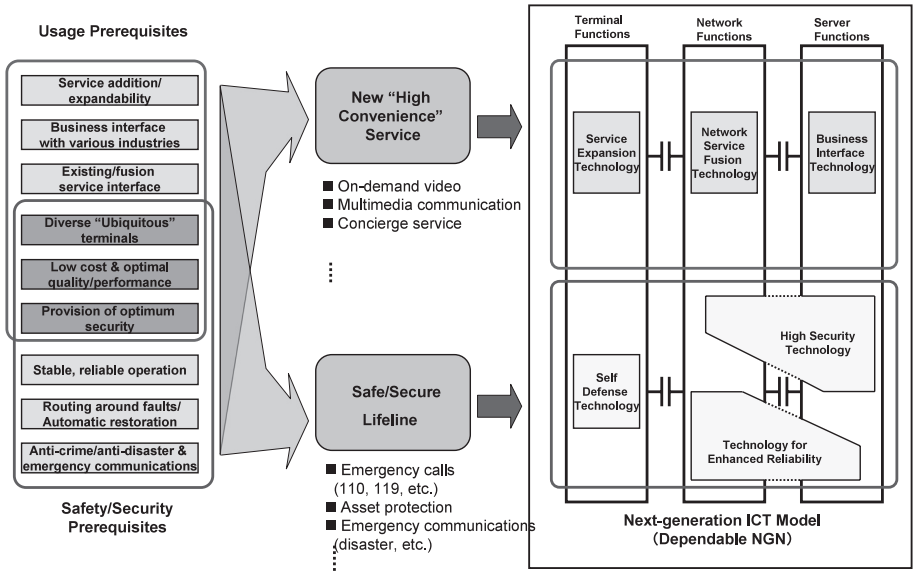


Fig. 3 Technological model for the next-generation Information & Communication Technology (ICT).

ter countermeasures, traffic control and operational management.

(2) IT System Technology Domain (2 papers)

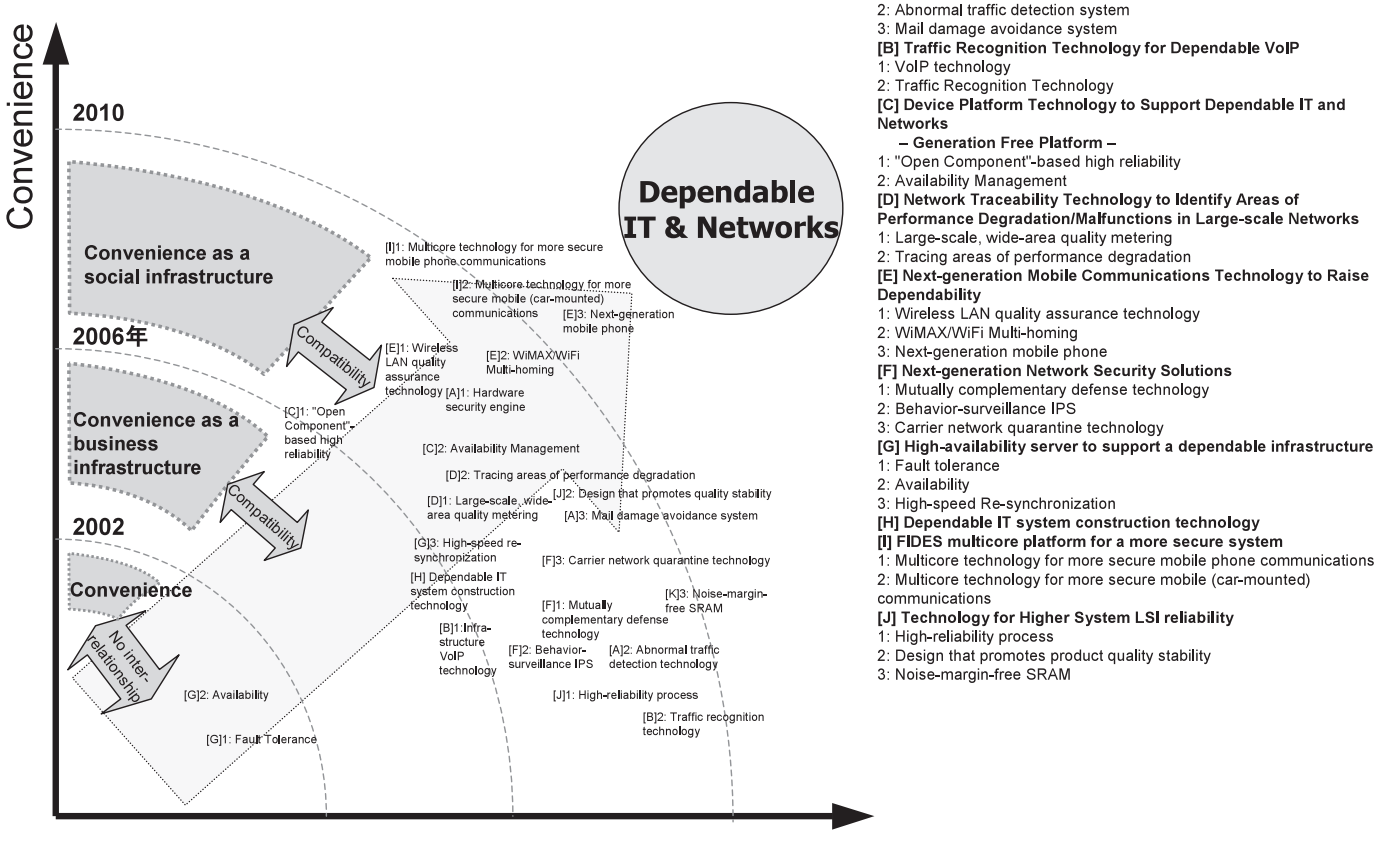
[G] In the paper of high-availability servers that support dependable infrastructure, we introduce fault tolerance, availability and high-speed synchronization. [H] In the paper of dependable IT system construction technology, we will explain system construction technology and developments that employs commodity products boasting excellent cost performance and that are premised on "fail safe" design to keep service downtime to an absolute minimum.

(3) System Device Technology Domain (2 papers)

[I] Our introduction of FIDES multicore platform technologies for a more robust and secure system puts the focus on non-symmetric multicore technology for mobile telephones and car-mounted systems as a technique to realize not only high performance and energy efficiency but also higher reliability. [J] In the area of developing system LSI with higher reliability, we introduce various technologies including semiconductor processing, design that promotes product quality stability, and noise-margin-free SRAM.

Fig. 4 maps technologies according to the 11 categories introduced in this special issue along the axes of convenience and lifeline characteristics. The dotted arcs indicate the approximate periods of time when the related technologies will be realized. NEC believes that each of these technologies is essential to the realization of dependable IT and networks, delivering both innovative convenience and safety and security.

This feature does not touch on many of the technologies that lie near the convenience axis and are already providing convenience as business infrastructure. Also with respect to convenience technologies in the social infrastructure, we plan to introduce them through our public relations communications and future issues of this publication as technologies to be deployed in a timely fashion based on consideration of market needs.



[A] Security Engine Technology to Provide a Dependable "Safe & Secure" Environment
1: Hardware security engine
2: Abnormal traffic detection system
3: Mail damage avoidance system
[B] Traffic Recognition Technology for Dependable VoIP
1: VoIP technology
2: Traffic Recognition Technology
[C] Device Platform Technology to Support Dependable IT and Networks
– Generation Free Platform –
1: "Open Component"-based high reliability
2: Availability Management
[D] Network Traceability Technology to Identify Areas of Performance Degradation/Malfunctions in Large-scale Networks
1: Large-scale, wide-area quality metering
2: Tracing areas of performance degradation
[E] Next-generation Mobile Communications Technology to Raise Dependability
1: Wireless LAN quality assurance technology
2: WiMAX/WiFi Multi-homing
3: Next-generation mobile phone
[F] Next-generation Network Security Solutions
1: Mutually complementary defense technology
2: Behavior-surveillance IPS
3: Carrier network quarantine technology
[G] High-availability server to support a dependable infrastructure
1: Fault tolerance
2: Availability
3: High-speed Re-synchronization
[H] Dependable IT system construction technology
[I] FIDES multicore platform for a more secure system
1: Multicore technology for more secure mobile phone communications
2: Multicore technology for more secure mobile (car-mounted) communications
[J] Technology for Higher System LSI reliability
1: High-reliability process
2: Design that promotes product quality stability
3: Noise-margin-free SRAM

Fig. 4 Technology map with convenience & lifeline characteristics as axes.

5 Conclusion

The achievements of NEC as a corporation that offers a broad array of IT and network technologies are entirely the result of the warm support and encouragement we have received from our customers both in Japan and around the world. In the coming era of the Ubiquitous Society, IT and network technologies will be converged. With the aim of realizing a highly advanced Information Society that will enrich lives, NEC will continue its endeavors across both the realms of IT and networks to develop and refine the technologies that make possible breakthrough hardware, software, and solutions that will serve our customers.

References

1) U.S.-Canada Power System Outage Task Force, "Final Report on the August 14th Blackout in the United States and Canada," April 2004. https://reports.energy.gov/
2) Northeastern North America Power Outage Research Group, "HOKUBEI HOKUTO-BU TEIDEN JIKO NI KANSURU CHOSA HOUKOKU," 14TH AUGUST, 2003 (Report on investigation about blackout in North-East region in North America on March, 2004)," http://www.enecho.meti.go.jp/denkihp/shiryo/nayousar2.pdf
3) CSI and FBI, "2005 Computer Crime and Security Survey," July 14, 2005. http://www.gocsi.com/
4) Akira Arutaki, Yoshihide Kikuchi, et al., "Technical Perspectives of the Construction of Dependable Network as the Social Infrastructure," The International Conference on Dependable Systems and Networks (DSN2005), Yokohama, Japan, June, 2005.
5) Akira Arutaki, Toshiyuki Kanoh, et al., "Construction of Dependable Network as Social Infrastructure", NEC GIHO, Vol.58, No.5 (September, 2005), pp.79-85 http://www.nec.co.jp/techrep/ja/journal/g05/n05/t050528.pdf
6) Ministry of Public Management, Home Affairs, Posts and Telecommunications, "White Paper 2005 Information and Communications in Japan" http://www.johotsusintokei.soumu.go.jp/whitepaper/whitepaper01.html