# Ubiquitous Security
## - Towards Realization of a Safe and Secure Digital World -

Katsumasa Shinozuka, President and CEO

This paper describes “Ubiquitous Security”, essential for realizing a “Ubiquitous Network Society” full of “Ubiquitous Services”.

In the coming Ubiquitous Network Society, real world and cyber world will be coordinated and converged by communicating with each “individuals” such as persons or objects connected to the network through RFIDs (Radio Frequency Identification) or sensor networks. The network safely and securely provides the best service for users without any ICT understanding or operation considerations on the users part by recognizing a person and the surrounding environment, while offering reasonable access to various information resources (information, database, content, services, etc.).

Ubiquitous Security identifies users and the surroundings properly to offer suitable services desired by “Individuals” safely and securely that “dynamically” change security levels according to the situation. The autonomous security control for the prevention of mobile phone theft is introduced as an example.

### Introduction

As stated in the presentations given at Telecom World 2003 and Telecom 99 Forum as well, the progress in Info-Communication Technology (ICT) has the potential to bring a networked information society in which “individuals” are in the leading role and everyone can live freely, fairly and safely, and that, ICT must fulfill the three vital functions[1), 2), 3), 4)]:

- Ensure “connectivity”, to provide communication “anytime, anywhere and to anyone”.
- Create new “services/contents” to enable use of “desired information in any form”.
- Ensure “security and reliability”, so the network will be “secure and reliable”.

Of these functions, “security and reliability” will be the vital subject for individuals to feel equally safe and secure using ICT.

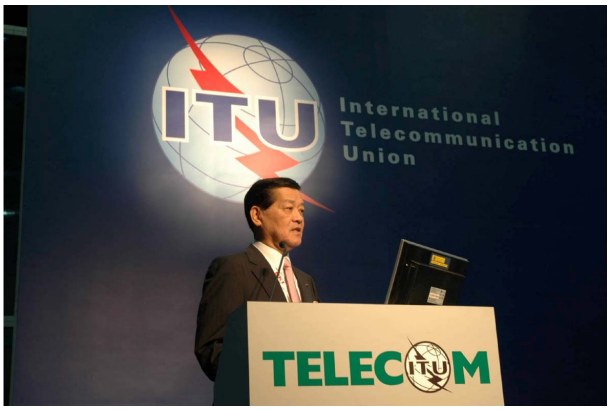


**Photo 1 Author on podium**
**(ITU Telecom World 2006 Forum in Hong Kong on December 7, 2006)**

ICT progress has enabled Japan to put in place a seamless mobile and broadband environment that is expanding globally, and “anytime, anywhere and to anyone” communication is close to reality. Furthermore, the creation of new “services/contents” for the use of “desired information in any form” is almost at hand.

However, behind the broadband society convenience exist threats and risks, such as increased cyber crimes, personal information leakage, and personal attacks and slandering over the network. There is also a problem of digital divide, a gap created when there are people who cannot enjoy the benefits of mobile and broadband environment due to lack of infrastructure deployment, or they are elderly or physically challenged and unskilled in ICT. For Japan, faced with low-birthrate and aging, the major goal is to solve these problems to create an enriched society where individuals equally and respectfully live a safe, secure, comfortable life.

The paper was presented at ITU’s TELECOM 2006 Forum.
The content of the paper is the opinion of the writer, and not the opinion of ITU.

## Ubiquitous Network Society in Japan

At first, the ubiquitous network society in Japan is described.

The chair's report from the United Nations at Tokyo Ubiquitous Conference in May 2005 stated, "A ubiquitous network society is a society where it is possible to seamlessly connect "anytime, anywhere, by anything and anyone", and to exchange a wide range of information by means of accessible, affordable and user friendly devices and services."[5].

Today in Japan, PCs, mobile phones, personal digital assistants (PDAs), and digital home appliances have penetrated everyday life. RFIDs, sensor networks, and other high performance processors are built into various "objects" and utilized in a variety of services both for businesses and homes. The ubiquitous society full of ubiquitous services is becoming a reality.

Faced with a rapid increase in the aging population and declining birthrate, Japan's top priority is converting from a mass production and mass consumption economy to a value-oriented economy based on advanced technology and refined cultural knowledge. The Japanese government initiated the e-Japan Strategy in 2001 to promote social structural changes by taking advantage of ICT. The goal was "to be the world's most advanced IT nation within five years." The e-Japan Strategy has progressed from the first stage of constructing a base infrastructure to the second stage of active IT utilization turning Japan into a world leading IT nation in broadband deployment, advanced mobile phone penetration, and electronic commerce and video delivery utilization. In 2006, the "new IT reform strategy" initiated proposes to "realize a society in which benefits of info-communications can be experienced anytime, anywhere and by anyone" by 2010 for Japan's international contributions and competitiveness[6]. The steps of Japan' IT strategy are shown in **Fig. 1**.

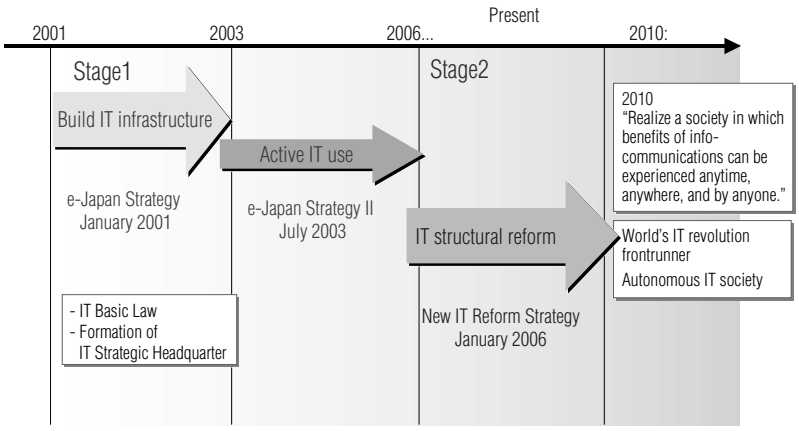


**Fig. 1 Japan's IT strategy**

Japan's current move towards the Ubiquitous Network Society can be categorized in one of two major trends.

The first trend is the construction of a ubiquitous broadband and mobile network environment.

As of June, 2006, 6.31 million households in Japan were subscribed to FTTH network and the total number of mobile phone subscribers has exceeded 90 million of which more than 30 million were third generation (3G) mobile phone subscribers[7]. Japan has the world's leading mobile broadband environment in terms of service penetration and price. Also, digital broadcast to mobile terminals (so called "one segment digital broadcast") in Japan was started in April of 2006, paving a way towards an environment where video services can be received on PCs, mobile terminals, TVs, and various other devices. As a result, legal and regulatory reforms and deregulations are currently under discussion for the convergence of telecommunication and broadcast environment. Furthermore, telecom carriers are leading the way in building a next generation network (NGN) infrastructure[8]. The goal is to create a "quadruple play" environment providing phone, TV, Internet and mobile application services over an IP (Internet protocol)-based platform through optical, wireless, CATV, broadcast and other media. RFIDs and sensors are also being embedded into "objects" in distribution, environment, manufacturing etc. for better efficiency, safety and security.

The second trend is the contents and service businesses deployment resulting from the ubiquitous network environment.

Due to the mobile phones' advanced features, mobile contents delivery of music and video, and use of mobile commerce is on the rise. In FY 2005, Japan's mobile contents market was 315 billion yen and mobile commerce market was 405 billion yen, a sharp jump of 21% and 57% compared with the previous year[7], respectively. Broadband has brought the collapse of the asymmetrical information flow, otherwise known as Web 2.0. Gone are the times when information was sent one-way from telecom carriers or contents providers. Individuals are now taking the lead role as consumers create their own contents and distribute them through blogs, SNS (social networking services), and video services. Increase in open source software holds the potential to drive value creation from sharing knowledge and collaboration, and to bring about a new work style that moves beyond corporate borders. Internet services such as net searches,

net shopping and net auctions connect producers and consumers directly unveiling small-scale markets and reducing mismatches.

## Visions of the Ubiquitous Network Society(e-Society®*1))

Ubiquitous Network Society is being realized through two major changes. They are progression of global seamless network and utilization of safe and secure mobile wireless network.

Until now, people themselves identified an object or environment that existed in the real world to decide and act. On the other hand, people accessed the cyber world through PCs, PDAs, mobile phones, and various other terminals. There was no coordination between the real world and the cyber world.

In the Ubiquitous Network Society, all surrounding objects have embedded computer chips of small-size, low power consumption, low cost, high performance that sense the environment, make decisions and communicate with others. As objects and environments in the real world are linked to the cyber world, human-to-object and object-to-object communications can be realized.

A person is identified through biometrics, while an object is identified by RFID as an "individual" distinguished from others. In addition, the network can detect autonomously a person's location or surrounding environment using video camera systems, environmental sensors, or positioning systems such as the global positioning system (GPS). The network can also monitor the person's health conditions and behavior through sensors placed on one's body.

As shown in **Fig. 2**, the network is capable of recognizing the context of a person, namely the situation or environment the person is in (context awareness), through a coordination and convergence between the real world and cyber world. Therefore, there is no need for individuals to be aware of his or her context (unconsciously).

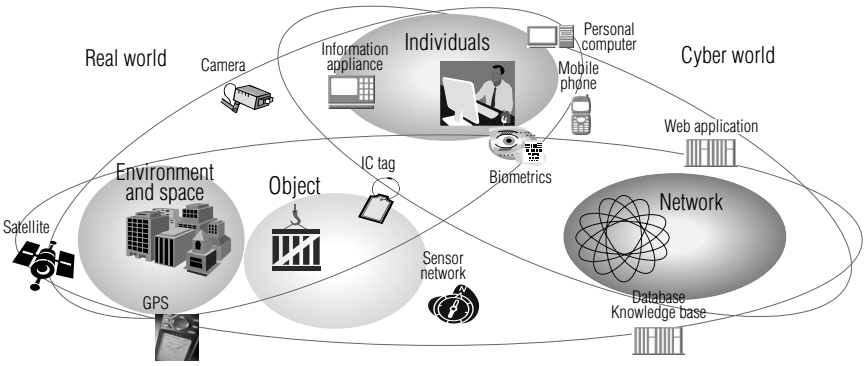


**Fig. 2 Coordination and convergence between real world and cyber world**

The progression of global networks, as well as secure wireless and mobile networks, make the ubiquitous network society a reality. The real world coordinates and converges with the cyber world in the Ubiquitous Network Society as networks become aware of persons and the situations they face (context awareness) while people no longer need to be aware of complex device operations (unconsciously).

## Ubiquitous Services

In the Ubiquitous Network Society, individualized "Ubiquitous Services" without any discrimination, can be offered supported by a context aware and unconscious network.

In the past, complicated operations were required to receive a service over the network. However, now, understanding the person's situation, the network can decide and provide the appropriate services for the user. In this way, without the user having special knowledge or skills for ICT and terminal equipment manipulation, people, young or old, handicapped or not, can all benefit equally from ICT enjoying the safe, reliable services.

Individuals can access the staggering amount of information resources that exist throughout the world to benefit from their desirable and most suitable services in a secure and safe manner without discrimination or restriction, according to the circumstances facing individuals, whether at the office, home or on the move.

Specific situations where ubiquitous services can be used are shown in **Fig. 3** and described below:

**(1) Finance**

A person is authenticated using advanced biometrics in place of PINs (personal identification numbers) or personal information registered in IC cards and payments for the trading transactions are accomplished without using any cash or checks.

*1) e-Society is a registered trademark of Oki Electric Industry Co., Ltd.

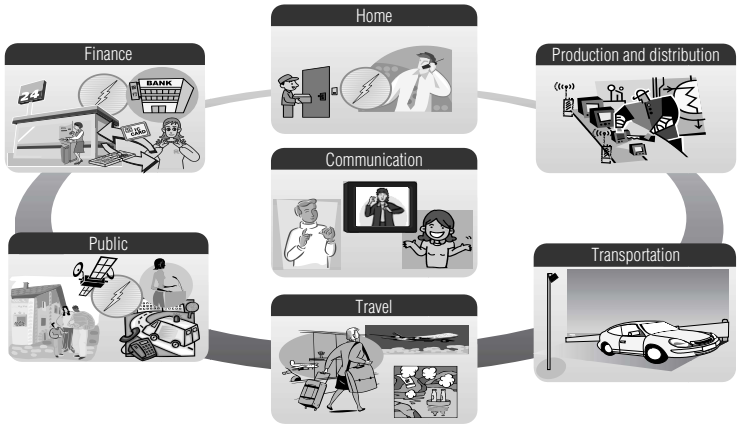


**Fig. 3 Situations for ubiquitous service use**

All individuals in the Ubiquitous Network Society, including the elderly, children and those with disabilities, can benefit equally from the services they desire using ICT in all situations, including at the office, home, public and communications.
Services are provided in modes most suitable for particular situations individuals face and such services can be received safely and securely.

**(2) Home**

Digital contents such as TV programs and movies will be viewed on-demand anytime, anywhere. Through the coordination of mobile phone network and home network, TV program or recorded contents being viewed on a mobile terminal outside will automatically switch to high-definition TV when the person enters a house.

**(3) Production/Distribution**

Objects tagged with RFIDs in factories and farms where a variety of environmental sensors are placed will be efficiently managed for product quality from production to distribution.

**(4) Transport**

With the availability of inter-vehicle and road-to-vehicle communications infrastructure, vehicle movement can be monitored to prevent collisions and to improve traffic flow thus creating a safe, energy efficient traffic system. The network will autonomously navigate people to their destinations taking into consideration the traffic conditions of the road.

**(5) Travel**

An integrated travel services such as planning, guides, tickets and hotel reservations, interpreter support and other required information are provided at a single stop.

**(6) Public**

When communication systems are down in a disaster such as earthquake or flood, an ad-hoc network will be established immediately for emergency communications to rescue people, guide evacuations and notify whereabouts of families as well as for normal communications.

**(7) Communication**

The network will detect the individual context and provide, in real-time, the necessary translation capability, whether it be voice-to-text, voice-to-Braille, sign-language-to-text or Japanese-to-English, so people can talk to each other without any difficulties.

## Threats and Anxieties in a Ubiquitous Network Society

Ubiquitous Network Society will provide ubiquitous services, which bring a more comfortable, convenient life to everyone, and people will be able to express their diverse individualities. On the other side, various threats and anxieties also come into existence as shown in **Fig. 4**.

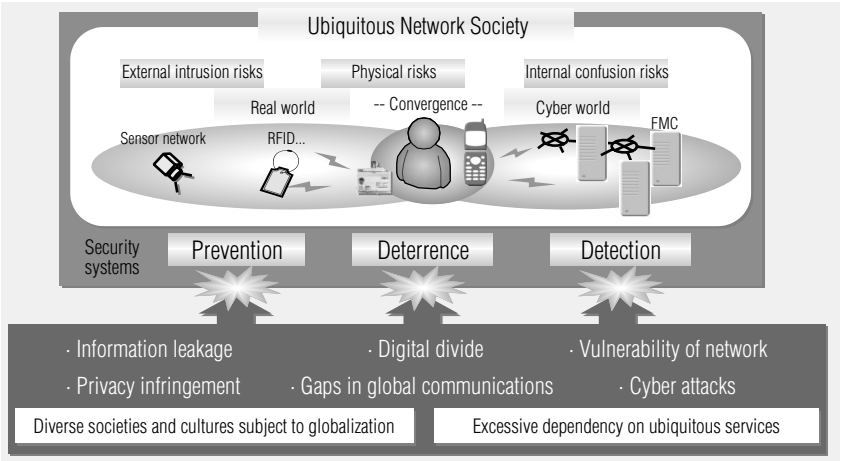


**Fig. 4 Threats and anxieties in ubiquitous network society**

The progression of ubiquitous services also brings about new threats and anxieties lurking behind the comfort and convenience.

- As functional supports from network increases, the risks from network vulnerability such as interruption in economic activities due to network outages will also increase (internal confusion risks).
- As functions and connectivity of devices enhance, viruses, spoofing and botnet may attack mobile terminals or sensors as well as once targeted servers or PCs (external intrusion risks).
- As volume of information handled by mobile terminals increases, loss of data and leakage of trade secrets or personal information will cause serious damages when those devices are lost or damaged (physical risks).
- Context aware services possess the danger of leading to privacy invasion and increase the anxiety of the end users.
- It is possible the problem of so-called digital divides such as differences in fulfillment of regional network environment or ICT literacy will expand.
- With a global seamless network, national boarders will be crossed deepening the understanding between people through the exchange of various cultures, customs and ideas, but this increased opportunity of exchange can give birth to new social and cultural misunderstandings and prejudices.

In order to realize a "true Ubiquitous Network Society" where a person can confidently enjoy the best available service, the elimination of these threats and anxieties are of utmost importance.

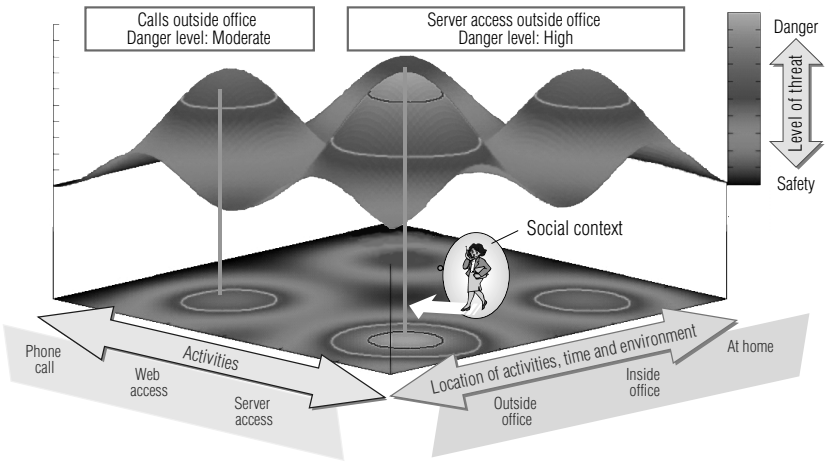


**Fig. 5 Threats and anxieties change depending on circumstances**

A dynamic security control that responds to situational changes is essential as threats and anxieties change depending on the location of an individual's activities, time, environment and details of the activities.

## Securities in a Ubiquitous Network Society

In the Ubiquitous Network Society, coordination and convergence between the real world and cyber world enable the understanding of user situations thus allows the offering of minute ubiquitous services. Threats and anxieties change, depending on the situations facing individuals and the type of services, that is "where" and "what". As shown in **Fig. 5**, for example, the level of threats and risks change depending on whether the user is working, commuting or on holiday, as well as whether the service is a phone call, browsing on the web or an attempt to access a server. A comparatively high level of security is required for gaining access to corporate internal servers from the outside.

Security functions in order to provide ubiquitous services safely and securely should respond to threats and risks that change with the situations facing individuals. Such a security is referred to as "Ubiquitous Security". Unlike the current "static" security, Ubiquitous Security identifies users and the surroundings properly to offer suitable services that "dynamically" change security levels according to the changing threats and risks without users having any ICT understanding or skills.

Examples of "ubiquitous security" are as follows. A summary is provided in **Table 1**.

- Security level of mobile phone will be determined autonomously according to whether the user is working, commuting or on holiday.
- A cyclist entering a poor visibility intersection will be warned if there is a vehicle approaching the intersection above a certain speed.
- If an earthquake occurs at a remote location, evacuation routes and methods will be given depending on the user's current position, time and behavior. The present whereabouts of family members will also be immediately notified.
- A person's vital signs can be constantly monitored, and if abnormalities such as in blood pressure or blood sugar levels are detected, warnings will be issued along with directions to the nearest hospital according to his/her location. In serious situations where the person may be incapacitated, emergency medical facilities will be contacted.

**Table 1 Examples of Ubiquitous Security services**

| | | |
|---|---|---|
| Autonomous Security Control | Context-based Mobile Security | · Detects/analyzes context (location, time, environment, etc.) using mobile phones.<br>· Recognizes threats (loss, theft, etc)<br>· Takes appropriate actions (notify, halt usage, delete data, etc.) |
| Health & Welfare Support | Pedestrian Guidance | · Detects with high precision the location of the pedestrian using the sensor network and mobile phone.<br>· Provides directions to the destination when the elderly or handicapped become lost or comes across disasters. |
| | Health Monitor | · Determines the physical and health status of a person by monitoring vital signs with a heart rate sensor, pedometer and accelerometer.<br>· In an emergency, contacts the medical center and calls for emergency vehicles using the sensor network and mobile phone. |
| | Airport Information | · Provides directions to facilities or locations within an airport using the sensor network.<br>· Provides evacuation/directional guidance during disasters.<br>· Autonomously navigate people with the support of under-floor RFID tags. |
| Disaster Prevention | Real-time Earthquake Detection | · Gives advanced notification of earthquake occurrences.<br>· Allows time to take measures before a big shock arrives. |
| | Others | · Local area disaster prevention support<br>· Emergency bulletins<br>· Communications with mountainous regions, remote islands, oceanic - vessels.<br>· Disaster information sensor network.<br>· Information analysis of disaster stricken areas using GIS (Geographic Information System). |
| Environment & Behavioral Recognition | Wireless Sensor Network | · Maintains a network comprised of sensor nodes that have sensor and wireless capabilities to recognize environmental features, such as position, temperature and humidity. |
| | Human Behavior Recognition | · Recognizes human behavior from images captured by roadside/store surveillance cameras and detects wait statuses or suspicious behavior. |

The context awareness functions for these services are shown in **Fig. 6** and also described below.

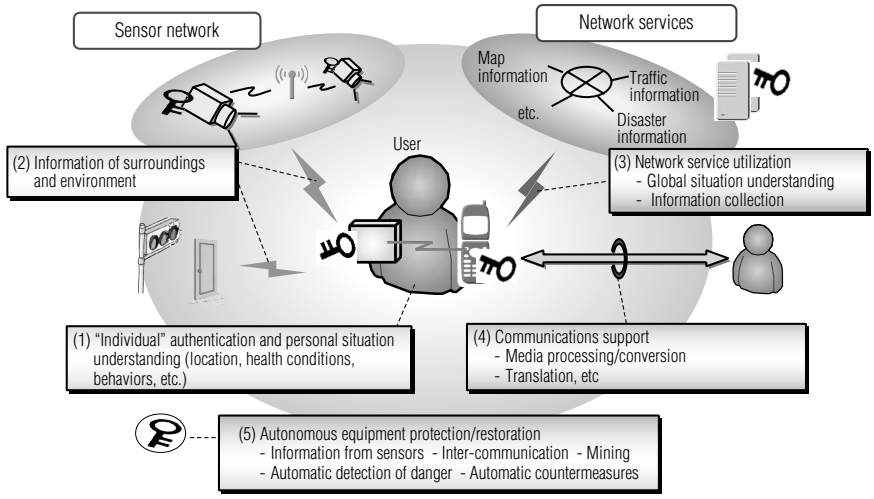


**Fig. 6 Five major contexts necessary for ubiquitous security**

**(1) User context awareness**

Biometrics technology will be applied to identify a person as the true user to prevent theft, snooping, false identities and other threats. Also information about the situations of the user such as behaviors and health condition will be obtained from sensors or terminals held by the user.

**(2) Environmental context awareness**

Numerous sensor nodes with wireless capabilities will be embedded in the environment and communicate with each other to obtain the information of the surroundings such as temperature, humidity, and accurate user location obtained by sensor networks and surveillance cameras etc. For example, information such as a car coming from the other side of the curve or burglar entering a home can be obtained.

**(3) Context awareness obtained from the networks**

This context awareness is based on information obtained from the network services. For example, with information from the network of traffic congestion at a remote location, people will be able to select a safe and suitable route.

**(4) Capability to detect communication gaps**

This capability is to detect communication gaps between persons or objects, point out that situation, and fill the gaps. In addition to the obvious translations of languages, it is also important to help people understand gaps related to cultural, literacy and other differences that they may unconsciously assume.

**(5) Network capability**

Lastly, the service infrastructure such as terminals, sensors and network should have the ability to recognize by themselves the situation and level of danger it is in. Additionally they should have the capability to autonomously and flexibly change its security levels in accordance with the situation.

Instead of increasing human responsibility, autonomous functions of the equipment and systems guarantee reliability and stability to prevent malicious attacks, maintain integrity of systems, and continue services.

## Example of an Autonomous Security Control for Mobile Phones

In this chapter an example of an autonomous security control for mobile phones utilizing context awareness technology developed by OKI[9] is described, which is referred to as context-based mobile security.

In the Ubiquitous Network Society, mobile terminals such as mobile phones and PDAs are the key devices for a person to obtain desired services from the network. These convenient devices also hold private and business information such as address books, emails contents, mobile wallets etc. Therefore, loss or theft of devices and leakage of information may cause considerable harm to the citizens of a Ubiquitous Network Society. It is essential to eliminate the threats and anxieties against theft and loss of mobile terminal devices.

The components needed for this security function are given below, as shown in **Fig. 7**.

① Mobile phone equipped with short-range radio and various sensors such as accelerometer, touch sensor, proximity sensor, and GPS, which gives information to the network of its location and status that the phone is moving or being held.

② The mobile phone owner also carries a small device called counterpart device (CPD) such as accessories, watches or business card cases, which contain the sensors same as the mobile phone.

The CPD and mobile phone communicate with each other to know the distance.

③ A management server in the network is also utilized to control the security policies of the mobile phone.

Next, the autonomous security actions are explained.

First, personal identity is authenticated with biometrics such as iris, fingerprint, and facial recognition to confirm the actual owner is carrying the mobile phone and CPD. Once identity is successfully authenticated, the autonomous security control mode is activated.

Assume an owner walks away leaving the mobile phone behind on the desk. The CPD and phone detects the distance between them are separating. They also notice the CPD is the one moving while the phone remains stationary. From this information, they consider the phone to be “left behind”. Security measures are then taken according to the “left behind” policy, for instance the CPD issues a voice warning, and the phone renders itself inoperable.

Take another example where a bag containing the mobile phone has been snatched away. Again, the separation between CPD and phone is detected. This time the phone is moving and considered as “stolen”. In this case, the phone immediately renders itself inoperable and emits a loud alarm.

Valuable data will be deleted if the “stolen” status continues beyond a certain period or someone other than the owner picks up the phone.

Additionally, with GPS information, the functions of the mobile phone can be restricted according to the security level in the area.

In such a manner, the mobile phone understands its own situation and autonomously set security levels following predefined rules, so the safety of the phone can be maintained without special attention from the user.

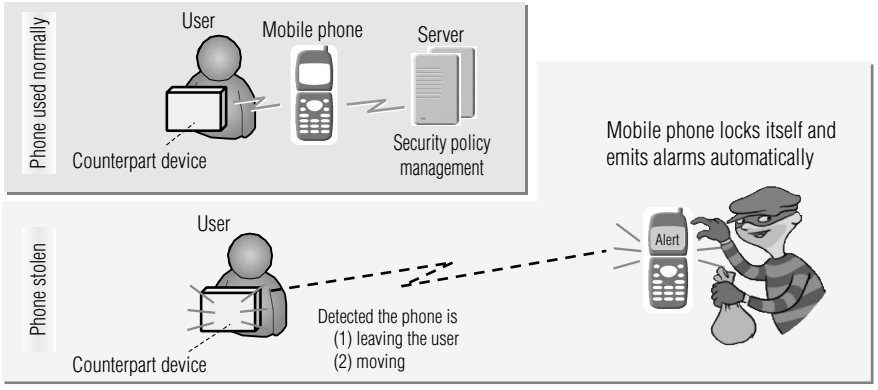


**Fig. 7 Example of ubiquitous security for mobile phones**

Context-based Mobile Security:
Using a mobile phone as well as a counterpart device equipped with various sensors and a short-range radio capability, it is possible to constantly monitor the status of the mobile phone to autonomously set the security level that is appropriate in response to the changing conditions of the mobile phone.

## Conclusion

This paper offered an overview of the ubiquitous services in the ubiquitous network society and the ubiquitous security to overcome threats and anxieties lurking behind convenience, for safe and secure ubiquitous services.

Ubiquitous Network Society is being realized through progression of global seamless network and utilization of safe and secure mobile wireless network. In the Ubiquitous Network Society, since all persons and objects are connected to the network as "individuals", the real world and cyber world will be coordinated and converged. The network can recognize individuals, their situation and the environment they are in, and provides the suitable services to users even while they are on the move, without the users having any ICT understanding or skills by changing security levels dynamically against threats and risks varied according to the situations.

Ubiquitous network citizens will equally access all the information in the world and understand the diverse languages, cultures and customs. People can express their own ideas and create new values by sharing knowledge with others in a trusted community.

We intend to press on with our efforts by orchestrating our wisdom and taking advantage of our partnerships to create the true "ubiquitous network society", or OKI's corporate vision "e-Society" full of ubiquitous services as shown in **Fig. 8**.

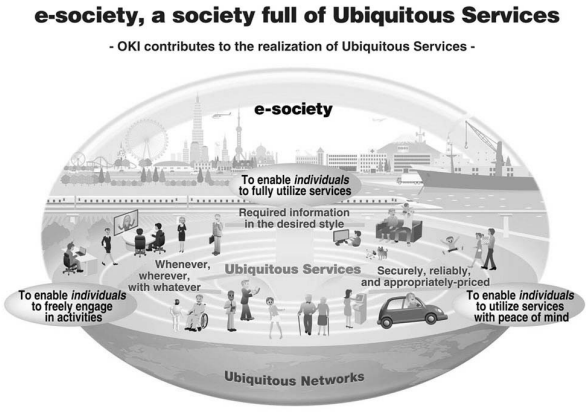


**Fig. 8 e-Society**

## References


1) Katsumasa Shinozuka: "Mobile Interactive Services: Risks and Solutions", ITU Telecom 1999 Forum Proceedings, October 1999.
2) Katsumasa Shinozuka: "Mobile Interactive Services: Risks and Solutions", Oki Technical Review, Issue 182, Vol. 67, No. 1, pp. 3 to 8, April 2000. http://www.oki.com/jp/Home/JIS/Books/KENKAI/n182/pdf/02.pdf
3) Katsumasa Shinozuka: "Building a Dependable Information Society Based on Broadband Networks", ITU Telecom World 2003 Forum Proceedings, October 2003.
4) Katsumasa Shizuoka: Building Reliable Information Society Based on Broadband Network, Oki Technical Review, Issue 197, Vol. 71, No. 1, pp. 4 to 9, January 2004. http://www.oki.com/jp/Home/JIS/Books/KENKAI/n197/pdf/197_R02.pdf
5) Ministry of Public Management, Home Affairs, Posts and Telecommunications: Summary on results of "Toward the Realization of a Ubiquitous Network Society", Ubiquitous Network Conference at Tokyo, May 2005. http://www.soumu.go.jp/s-news/2005/pdf/050517_4_01.pdf
6) IT Strategic Headquarters: "New IT Reform Strategy", January 2006. http://www.kantei.go.jp/jp/singi/it2/kettei/060119gaiyou.pdf
7) Ministry of Public Management, Home Affairs, Posts and Telecommunications: White paper on "Information and Communications in Japan 2006", July 2006. http://www.johotsusintokei.soumu.go.jp/whitepaper/ja/h18/index.html
8) NTT: "Promoting NTT Group's Medium-Term Management Strategy", November 2005. http://www.ntt.co.jp/news/news05/0511phqg/051109.html
9) Koyama and Mitsui: "Aming to Realize Safe and Secure Mobile Phones", Oki Technical Review, Issue205, Vol. 73, No. 1, pp. 12 to 15, January 2006. http://www.oki.com/jp/Home/JIS/Books/KENKAI/n205/pdf/205_R14.pdf



**Photo 2 A Forum session scene (Presentation DS-13 on "Towards a Safer Digital Society" on December 7, 2006 in Hong Kong.)**