



www.ddsi.org

National Dependability Policy Environments

JAPAN

Report Version: Final
Report Preparation Date: 1 November 2002
Classification: Public
Preparation led by: RAND Europe (NL)

Contract Start Date: 1 June 2001 Duration: 18 months
Project Co-ordinator: RAND Europe (NL)

Partner: RAND Europe (NL, Project Coordinator); King's College London (UK);
Cell Network (S); IABG (D); Almaweb (I); LINK (P); ELIAMEP (GR);
Ernst Basler + Partner (CH), Isdefe (E)



IST-2000-29202

Project funded by the European Community
under the "Information Society Technology"
Programme (1998-2002)

Table of Contents

Overview of the Country’s Information Infrastructure	3
Main ICT Regulatory and Legal Developments	4
Assessment of Phenomena Undermining Dependability	5
Government Initiatives Aimed at Tackling Cyber-Security	6
Industry and Other Non-Government Activities Related to Dependability	8
Public-Private Partnerships	9
Research and Development	9

Overview of the Country's Information Infrastructure

Japan has been consistently ranked as one of the world's best-prepared countries for e-commerce. May 2000 figures from the Ministry of Post and Telecommunications (MPT) put Japanese Internet users at 27.06 million, which is 21.38 percent of the overall population. Following government stock deregulation in 1999, e-commerce began to flourish. However, as might be imagined for a country that prides itself on its technological innovation, Japan is somewhat paranoid about getting left behind. An Electronic Commerce Promotion Council of Japan (ECOM) was set up in 1995 as part of the Ministry of Economics, Trade, and Industry (METI) which acts as a focal point for all information concerning e-commerce in the country. ECOM has also been overseeing a number of test-bed projects and pilot studies related to e-Commerce across Japan.¹

However, according to the Economist Intelligence Unit (EIU), Japan still faces problems in becoming 'e-ready': in 2000, this nation came in 21st in rankings of the countries most prepared for e-business. This is largely due to the business environment, regarded as much less entrepreneurial than that of the West.²

Many experts believe that the key to the full development of e-commerce will be through mobile means, given the massive penetration of mobile telephony and Internet in the country. However, the cost of mobile Internet access is still considerably high.

In terms of infrastructure, Japan is thought to lag behind the United States by about three years. 7 million computers were sold in 1997, with 48 million computers sold in 2000. It has been projected that 54.65 million computers would have been sold by the end of 2001.³ ICT contributed 5 percent to the GDP in 2000⁴ and 6.2 percent in 2001.⁵ As at the end of 2000, there were 27,060,000 Internet users, with 36,300,000 households with computers. This resulted in a total of 47.08 million over all users.

Investment in telecommunications infrastructure amounted to US\$30,829 million (EUR 34,327 million). B2B e-trade was ¥8.62 trillion (EUR 74.75 billion) in 1998 and was projected to be ¥68.4 trillion (EUR 593 billion) by 2003. B2C e-trade was ¥64.5 billion (EUR 559 million) in 1998 and ¥248.0 billion (EUR 2.15 billion) in 1999, with ¥3.5 trillion (EUR 30.35 billion) projected for 2003 and ¥5.5 trillion (EUR 47.7 billion) for 2004.⁶ Wireless penetration stood at ¥54.1bn (EUR 469 million) in 2000, with ¥1,719 billion (EUR 14.9 million) projected in 2005. There are currently approximately 4 million subscribers via NTT/DoCoMo/ i-Mode.

Certainly, investment in this infrastructure is seen as important in revitalising Japan's somewhat moribund economy. To this end, former Prime Minister Keizo Obuchi published a 'Millennium Project' in October

¹ www.ecom.or.jp/ecom_e/index.html

² United States Internet Council and ITTA Inc, *State of the Internet 2000*: usic.wslogic.com/section4.pdf

³ www.c-i-a.com/200107cu.htm

⁴ UBS Warburg, *Global Economic Perspectives* (14 June 2001): www.ubswarburg.com/e/images/pdf/theme3.pdf

⁵ Robert H. McGuckin and Bart van Ark, *Making the Most of the Information Age: Productivity and Structural Reform in the New Economy*: www.conference-board.org/products/researchreports/dpubs.cfm?pubid=R-1301-01-RR

⁶ www.ecom.or.jp/ecom_e/report/no7/wg21.html

1999 as the strategy to propel Japan into the Information Society, chiefly by the establishment of a unified high-speed fibre-optic network by 2005.

In January 2001, the office of the Prime Minister (Kantei) published its e-Japan plan which put forward the need for the country to take revolutionary yet realistic actions to create a knowledge-emergent society. The plan stipulated that Japan would become the most advanced IT nation within 5 years. The high-speed fibre-optic network mentioned above is one of the targets in the plan. Always-on access for all citizens is also put forward by 2002.

Government departments and agencies centrally involved in e-commerce are the Ministry of Economics Trade and Industry (METI) with its Electronic Commerce Promotion Council of Japan (ECOM), the Centre for the Informatisation of Industry of the Japan Information Processing Development Centre (JIPDEC CII), and the Japan e-Commerce and Continuous Acquisition Life Cycle Support (JECALS).

In 1998, METI invested ¥80 billion (EUR 6.9 million) in e-commerce projects. By 1999, there were over 200 projects under way. Two reports were published which highlighted efforts in promoting e-commerce amongst industries in Japan. These were firstly the 'Outline of the Advanced Information System Development Testbed Projects', as well as an 'Outline of the Industrial and Social Information Infrastructure Development Projects'.⁷ Japan has committed itself to the development of e-government by FY 2003. Network security has been recognised as being essential for secure e-government.

Main ICT Regulatory and Legal Developments

In 1985, the telecommunications sector was fully deregulated and the main player, Nippon Telephone and Telegraph Corporation (NTT) was privatised in the first info-communications reform phase. Measures to promote network communication were in the second phase of info-communications reform in 1999. There are now over 8,700 new entrants in the sector, which has resulted in a diversification of services and reduction in charges due to increased competition. The Japanese government has firmly placed itself on the road to pro-competitive regulatory reform of this sector.

Major pieces of legislation in this area include the Telecommunications Business Law, the Law Concerning Nippon Telegraph and Telephone Corporation, the Radio Law, the Broadcast Law, and the Cable Television Broadcast Law. All industry self-regulation of the sector is accomplished by the Telecommunication Technology Committee (ITC), contributing to the promotion of standards for telecommunications terminal equipment and networks. The Japan Approvals Institute of Telecommunications Equipment has responsibility for certification of telecom terminal equipment. Convergence has not yet been addressed by the Japanese government.

Most telecom and Communication Service Provision (CSP) services are open to competition; however, foreigners or foreign-owned companies are not allowed to a licence for broadcasting (either via television or AM/FM radio). Some of the key areas for government action in e-Japan include a drastic review of regulation in the telecommunications industry, a shift in the regulatory perspective, stricter supervision over anti-competitive acts by the dominant carriers, and the establishment of a body for telecommunications competition arbitration.

⁷ [Current State of Business to Business Electronic Commerce in Japan – Report of JECALS \(1999\): www.jecals.jipdec.or.jp/wwwE/report-final1.pdf](http://www.jecals.jipdec.or.jp/wwwE/report-final1.pdf)

Similarly, with regard to e-commerce, the Japanese government is looking to pursue aggressively e-commerce opportunities throughout 2002 by revising regulations pertaining to e-commerce, clarifying existing regulations, and legislating for new rules (e.g., digital signatures) for contracts and protection of consumers.⁸

Decisions regarding the export of cryptography are made on an individual case-by-case basis under the terms of the 1998 Wassenaar Arrangement's General Software Note. However, businesses require approval for any exports larger than ¥50,000 (EUR 431). Law on electronic signatures generally follows principles laid down in the EU Directive on Electronic Signatures, which mandates non-discrimination between electronic and physical signatures and also puts forward a scheme for voluntary accreditation for service providers.

ECOM's Certification Authority (CA) Working Group released guidelines in 1997 proposing a set of widely generalisable standards for the requirements for certificate authorities. CAs are split into 3 levels, depending upon the level of assurance required.

In November 1999, the Ministry of Justice's Working Group on Legal Aspects of Electronic Commerce published a report on a legal framework for electronic certification and authentication services in Japan. The Group suggested that electronic signature systems should be based upon existing commercial registration and notarisation schemes.

On 1 April 2001, the Law Concerning Electronic Signatures and Certification Services came into force. This places electronic signatures on the same legal footing as physical signatures and aids the e-Japan priority policy area of 'facilitation of e-commerce'.

The target for the achievement of e-government in Japan is 2003 and targets within this include the digitisation of public administration within central and local government, digitisation of public services to the private sector, the publication of administrative information via the Internet, and support for local government ICT programmes.

Assessment of Phenomena Undermining Dependability

The Japanese are becoming increasingly aware of information security threats undermining dependability, trust, and confidence in the Internet economy. With the adoption of e-commerce plans and the subsequent realisation of the economic benefits that e-Commerce can bring, the Japanese government is acutely aware of the need to maintain trust and confidence in on-line commerce.

In 1999, there were 2,965 cases reported to the NPA (National Police Agency); this rose to 11,135 for 2000. Out of this figure, 2,896 were concerned with illegal and harmful content, 1,884 were defamation, 1,396 were fraud-related, 1,352 were unsolicited e-mail, 1,301 were concerned with illegal Internet auctions, and 2,306 were other 'unspecified' crimes. Between January and July 2001, 17 offenders were arrested, the majority obtaining the user ID and password combination from an acquaintance who had not kept them private.

However, the importance of protecting Critical Infrastructure is only just becoming a priority for the Japanese. This should be an especially important area for them, as they are highly-reliant on imports for social, economic, and national well-being.

⁸ E-Japan Summary available at: www.kantei.go.jp/foreign/it/network/0122summary.html

Japanese authorities have identified the threats that may affect critical infrastructures in the future. The Ministry of Economy, Trade, and Industry's (METI already identified) Office of IT Security Policy (a department within the Office of IT Planning), has identified dangers as stemming from traditional threats to information such as privacy, reliability of services dependent on IT, data leakage from personnel, and operational misuse. Japanese officials are keen to stress the lack of control over the communication-line, which can lead to a variety of threats at different stages of an electronic communication between two physically remote parties. This analysis splits up the process into three areas of concern: the security of the sender's personnel/hardware and software, the communication-line and the security of the receiver's personnel, and hardware and software. Threats at either end of the process include illegal operation by the user, hardware and software bugs present in programs and applications, as well as corporate information leaks. The communication stage has threats relating to eavesdropping, denial of service attacks, impersonation of user identity, and theft of proprietary information and content.

Responsibility for control of this intermediate state is impossible to apportion. Such responsibility is easier to manage in a system where the communication channel is owned by one company (e.g., telephone, fax, etc.) but as the Internet is a global network of networks, this is significantly harder to do.

Recent instances of hacking activity in Japan include buffer overflow attacks against a number of Japanese government web-servers, as well as defacement of the Science and Technology Agency, and the Ministry of Transport homepages.

Government Initiatives Aimed at Tackling Cyber-Security

The government has put forward a number of efforts to mitigate the threats posed by cyber-criminals and cyber-terrorists. An 'Action Plan for Building a Foundation of Information Systems Protection from Hackers and other Cyber-Threats' was published in January 2000. 'Guidelines for IT Security Policy' were issued in July 2000 and a 'Special Action Plan on Countermeasures to Cyber-Terrorism of Critical Infrastructure' was published in December 2000. The January 2000 Action Plan proposed that 'Guidelines for IT Security Policy' should be adopted by December 2000. Furthermore, it mandated that each ministry and agency should establish its own IT security policy by the end of FY 2002. As a result of a major spate of ministerial web-site defacements, the deadline for the creation of a security policy was moved to December 2000.

Individual ministry and agency guidelines are to be based on the Guidelines for IT Security Policy, which contain specific physical, human (composed of training, education, and password management issues), and technical security, as well as operational issues.

An 'Unauthorised Computer Access Law' was passed in February 2000. This law focuses on the 'prevention of high-tech crime and maintenance of the order of electrical communication'. This is necessary for the 'sound growth of advanced information communication society'. Sentences include a fine of not more than ¥300,000 (EUR 2,586) for facilitation of unauthorised computer access and a similar fine or prison sentence for up to a year for unauthorised access.

A law concerning Electronic Signatures and Certification Services was passed in May 2000, giving legal ground for the treatment of electronic signatures at the same standards as physical signatures.

Tax concessions have also been implemented for those organisations that have installed firewalls and anti-virus software in an effort to improve the state of security of many private firms in Japan.

Public safety commissions have also been given a role in emergency response to computer attacks. Information-sharing with a number of official agencies (National Public Safety Commission NPSC, METI, and the Ministries of Public Management, Home Affairs, and Posts and Telecommunications) is also put forward under the heading of protective measures.

Public awareness efforts include the establishment of general IT Security Countermeasures Council and an IT Security Community Centre.

Finally, with a view to the creation of secure e-government, frameworks against cyber-crime and cyber-terrorism have been published. Under the framework against cyber-crime, High-Tech Crime Technology Divisions and High-Tech Crime Technology Support Centres were established within each Divisional Centre of the NPA in April 2000. These units provide liaison, co-ordination, and technical advice to the Prefectural police.

In April 2001 a Counter-Cyber-Terrorism Technology Office within the High-Tech Crime Technology Division of the NPA was established under the 'Framework against Cyber-terrorism'. A Counter-Cyber-Terrorism Unit was also established within the NPA, to co-ordinate with the Critical Infrastructure owners and collect information about terrorist organisations.

The special action plan on countermeasures to cyber-terrorism of critical infrastructure is a major policy document which marks Japan's identification of Critical Infrastructure Protection as a major theme. The stated goal is to protect the telecommunications infrastructure upon which businesses and peoples' lives increasingly depend.

The critical sectors have been identified as telecommunications, finance, aviation, railroads, electrical power, gas, and government/administrative services (including regional public organisations). To mitigate or reduce the threats to these sectors, the next stage is to execute a risk assessment and implement protective measures to raise the security level according to the relative importance of each system.

Co-ordination and communication between the private sector and government need to be set up and monitored for the prevention, response, and sharing of security data and warning information. Co-operation must also be established between the private and public sectors for detection and emergency response to cyber-attacks. The plan also called for government to work towards establishing the foundations of information security in relation to personnel training, R & D, and appropriate regulation for the development of further countermeasures against cyber-terrorism. International co-operation plays a big part in the Special Action Plan, which calls for the promotion of international co-operation due to the international nature of cyber-attacks. Finally, the Action Plan contains a statement that it is a working document and as such will come under review.

As of September 2001, there were two Certification Authorities (CAs) up and running for e-government (a Bridge CA and a Ministerial CA) with local government CAs planned. The Ministry of Justice has been overseeing an Electronic Authentication Registry which is partly operational. Private CAs are also operational for individuals, with accreditation based on recently-passed legislation.

Japan has been an active participant in the development of ISO 17799 and has been cognisant of OECD guidelines on information security and cryptography. Japan has also played a role in the Convention on Cyber-crime and G8 discussions relating to the threat of cyber-terrorism and cyber-crime.

Industry and Other Non-Government Activities Related to Dependability

There are a large number of active foundations in Japan concerned with the development of an e-society and e-business. They are usually industrially-backed associations, although there are a number of academic bodies doing work into cryptography and standards. One of the main organisations is the METI-backed IPA (Information Technology Promotion Centre)-ISEC (Information Technology Security Centre), which was established in 1997, issues alerts, and conducts activities for the promotion of a secure information infrastructure. Expectations are that significant work will be done in the public-private policy implementation of any critical infrastructure protection work that will appear.⁹

Others include the Japan Information Processing Development Corporation (JIPDEC)¹⁰, the New Media Development Association (NMDA),¹¹ the Internet Association of Japan (IAJapan),¹² and the Centre for Information on Security Trade Control (CISTEC).¹³ Other relevant organisations include the Japan Network Security Association (JNSA),¹⁴ the Electronic Commerce Technology Research Association (ECSEC),¹⁵ the IT Security Centre of the Japan Electronics and Information Technology Industries Association (JEITA/ITSC),¹⁶ the Information Technology Research and Standardisation Centre (INSTAC),¹⁷ the Information Processing Society of Japan (ISP-J),¹⁸ the Japan Society of Security Management (JSSM),¹⁹ and the Technical Group on Information Security of the Institute of Electronics, Information and Communication Engineers (IEICE).²⁰

A Computer Emergency Response Team Co-ordination Centre (JPCERT/CC) was set up in 1997 as an independent body, has an advisory role, and liaises with computer system administrators at network sites, as well as with supporting service providers and equipment vendors. The Centre also runs an electronic mailing list of security information.²¹

⁹ Information Technology Security Centre – Information Technology Promotion Agency: www.ipa.go.jp/security/index-e.html (downloaded 28 January 2002)

¹⁰ Japan Information Processing Development Corporation: www.jipdec.or.jp/kyotu_page/outline.htm (downloaded 28 January 2002)

¹¹ New Media Development Association: www.nmda.or.jp/index-english.html (downloaded 28 January 2002)

¹² Internet Association of Japan: www.iajapan.org/index-en.html (downloaded 28 January 2002)

¹³ Centre for Information on Security Trade Control: www.cistec.or.jp/open/intro/cistec/generalinfo.html (downloaded 28 January 2002)

¹⁴ Japan Network Security Association: www.jnsa.org/english/index.htm (downloaded 28 January 2002)

¹⁵ Electronic Commerce Technology Research Association: www.ecsec.org (downloaded 28 January 2002)

¹⁶ IT Security Center of the Japan Electronics and Information Technology Industries Association: www.it.jeita.or.jp/infosys/itsec/index.htm (downloaded 28 January 2002)

¹⁷ Information Technology Research and Standardisation Center: www.jsa.or.jp/INSTAC (downloaded 28 January 2002)

¹⁸ Information Processing Society of Japan: www.ipsj.or.jp (downloaded 28 January 2002)

¹⁹ Japan Society of Security Management: www.jssm.net (downloaded 28 January 2002)

²⁰ Technical Group on Information Security of the Institute of Electronics, Information and Communication Engineers: www.ieice.or.jp/ess/ESS/tg-e.html (downloaded 28 January 2002)

²¹ Computer Emergency Response Team Co-ordination Center: www.jpCERT.or.jp/english (downloaded 28 January 2002)

Public-Private Partnerships

The Japanese have only recently considered the idea of public-private partnerships. However, experts agree that the Japanese industry has a healthy relationship with government that may be conducive to further targeted regulation and participation in certain areas. Certainly, the Japanese government is not averse to intervening when it thinks it necessary. However, it remains to be seen whether the bureaucratic nature of doing business will hinder the development of e-commerce, which relies upon an open and (as much as possible) unregulated market.

The overall assessment is that little work has been done in establishing functioning public-private partnerships in Japan, although the necessity of doing so for the establishment of e-commerce and e-Japan has been recognised. At the moment, the situation is split between competing industry-backed bodies and associations, government agencies such as the IPA, and independent organisations such as JPCERT/CC.

Research and Development

Japanese government R&D is focusing on four main areas. These are research into key technologies for network security (network, contents, access and other common technological developments); highly-reliable back-up systems; technology to detect network failure (detection of levels of traffic, status, and load on portions of the Internet); and finally, technology to trace unauthorised computer access.

Standardisation and the drive towards a government PKI (GPKI) are also areas where Japanese public bodies, under METI are conducting research. A Next-Generation Internet Zone Promotion Association (under the MHCPT) was established in 1999 with a view to the provision of education and outreach and assistance for the creation of a Next-Generation Internet Society. This is a collaborative partnership, relatively unique in Japan, which sees private sector, academia, and administrative bodies collaborating on Next-Generation Internet (NGI) discussions.

A pilot project of an Internet cash payment system (ICASH) has been underway since September 1998 under the auspices of the Cyber Business Association (CBA).²² Other projects funded by the MHCPT include technology for ultra high-speed data transmission and bandwidth usage, digital watermark technology, technology for the authentication of web-sites, technology for secure and reliable transmission of data (such as electronic money), and technology for the provision of a highly-reliable Internet and the availability of bandwidth.

An exotic plan for the provision of Internet services via unmanned airships was also conceived in 1998. Christened Sky-Net, this plan was begun in co-operation between the Science and Technology Agency and the MHCPT. Other large-scale projects include the Japan Gigabit Network, a project of the Telecommunications Advancement Organisation of Japan.

Several pilot projects have also been initiated by METI with government funding. Work has also been underway with standardisation, particularly with regard to the International Telecommunications Union (ITU) and the International Standards Organisation (ISO).

²² Cyber Business Association: www.fmmc.or.jp/associations/cba/index.html (downloaded 28 January 2002)