

**Cyber Rules: The Rules  
Governing E-Commerce  
and the Challenges Facing Japan**

**Takeshi SHINOHARA**

**Nomura Research Institute**

# Cyber Rules: The Rules Governing E-Commerce and the Challenges Facing Japan

Takeshi SHINOHARA

- I Cyber Rules in the Limelight
  - 1 Cyber Rule Problems in the Past
  - 2 Current Cyber Rule Problems
- II Cyber Rule Systems
- III Structure of Rule Governance
  - 1 Self-Regulation, Government Regulation and the Technological Approach
  - 2 Role of the Private Sector, Government and International Organizations
  - 3 Regional Models of Governance in the US, Europe, and Japan
  - 4 Are Cyber Rules Going to Converge As a Single-Rule Model?
- IV Issues Facing the Japanese Government and Japanese Companies

As electronic commerce via the Internet (“e-commerce”) has grown, so has the realization of the importance of the various rules governing e-commerce (“cyber rules”). Because most of the current commercial rules take no account of the specific nature of e-commerce, situations arise that the current system had never envisioned or in which the rules even impede the development of e-commerce.

By its very nature, e-commerce is a global phenomenon unrestricted by national boundaries. Therefore cyber rules must also be global. This paper considers the kind of cyber rules needed in nine different areas: (1) contract validity and digital certification; (2) consumer protection; (3) the protection of privacy; (4) security; (5) taxes and customs duties; (6) intellectual property rights; (7) business model patents; (8) Internet domain names; and (9) intermediary responsibility.

There is also the issue of who should be responsible for devising cyber rules and how they should be determined (“rule governance”). This paper analyzes the structure of governance from the following four points of view: (1) the kind of changes that are taking place in terms of self-regulation (voluntary regulation by industry), statutory regulation and the technological approach; (2) the changing roles of the private sector, government and international organizations; (3) the main features of the governance models used in the United States, Europe and Japan; and (4) the question of whether global cyber rules are going to converge as a single-rule model or interact as a multiple-rule model.

The paper assumes three possible scenarios for the changing structure of cyber rule governance: (1) increasing globalization; (2) a revival of the authority of the nation state; and (3) changes in the features of market capitalism. Inevitably, changing rules can be expected to lead to the emergence of numerous and diverse global platforms.

If Japan is to recover the ground it has lost in this area, it urgently needs more people capable of determining cyber rule policy and the markets in which it is applied. And because the private sector leads the way, political and administrative systems need to be reformed to allow the private sector to play a greater role.

# I Cyber Rules in the Limelight

## 1 Cyber Rule Problems in the Past

This is not the first time the rules for global network commerce have come up for discussion. In the field of finance, UNCITRAL (the United Nations Commission on International Trade Law) has been the venue for examining the division of responsibility between payers and payees in electronic funds transfers (EFT), while discussions about rules for electronic data interchange (EDI) have been continuing for many years in forms dealing with trade.

One example of international disagreement over such rules is the objections that were raised in Europe to cross-border data flows when General Electric entered the international market for time-sharing services in the early 1970s. These protests were based on the grounds that the arrival of a US online service provider in Europe would lead to a concentration in the United States of data on European individuals and companies, thereby threatening privacy, national defense, and industrial policy in Europe.

## 2 Current Cyber Rule Problems

Compared with the problems that surrounded cyber rules in the past, those that we face today are clearly more complicated, and they emerge more quickly. As indicated in Figure 1, this is the direct result of the explosive growth of the Internet since 1995. At the moment, Internet usage is still doubling every 12 months, and this has had the following effects on cyber rules.

### (1) The increasing number of Internet users

The first of these effects is the increasing number of people and companies using the Internet. Underlying this is the key feature of the Internet: the fact that it enables

every user to communicate with any other user. This has led to a number of social problems that would not have arisen if the Internet had still been the preserve of only a small number of specialists. These include issues such as protecting consumers, removing harmful content, ensuring security, and the means of settling disputes.

The situation is complicated by the fact that these are cross-border issues that cannot be dealt with solely by national law. One example is the problem of how to levy taxes on international transactions.

### (2) The emergence of broadband communications

Increasing bandwidths (i.e., more capacity) have made it possible to digitally transmit various media such as visual and musical content. While this is creating new business via the Internet, it has also begun to create major new problems involving intellectual property rights. In short, technical advances have helped to create a bigger market, but have led to the emergence of problems that cannot be controlled by systems and technology alone.

The vertical axis in Figure 2 shows the expansion that has taken place in communications bandwidth. As a result, services that used to be regarded as non-tradable goods can now easily cross borders. One example of this in Europe is the fact that call centers tend to be concentrated in Ireland and Britain. Similarly, some of India's outstanding software specialists can develop software for companies in the United States by using international communications lines.

The horizontal axis, on the other hand, shows the amount of communications consumption required to carry out a transaction. Increasing communications capacity not only involves greater bandwidth requirements but also creates new types of transactions, such as online auctions and messaging services as the cost of being permanently online has declined.<sup>1</sup> One example of this is Gnutella—a very recently developed type of software for swapping music online that has had a profound impact on cyber rules.

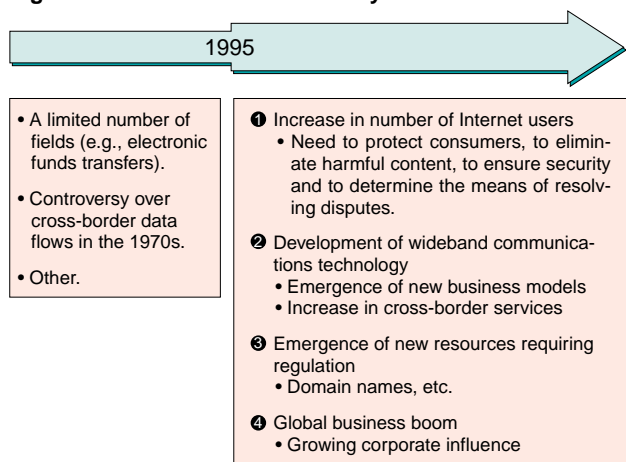
Given that communications capacity is due to increase a thousand-fold over the next 10 years, the developments shown in Figure 2 have only just begun.

### (3) The emergence of new resources

The emergence of new resources in cyberspace has meant that rules are now needed for controlling them. One example of this is Internet domain names.<sup>2</sup> The days when domain names could be obtained on a first-come-first-served basis are long passed. Indeed, domain names themselves have acquired a value, and problems have arisen because of confusion and competition with actual trademarks. As a result, the rules governing these names need to be reviewed and means found for settling disputes.

A scramble has also begun for business model patents, which are seen as a new cyberspace resource, and

Figure 1. Pre- and Post-Internet Cyber Rules



the need for new rules to deal with this has become apparent.

**(4) Growing influence of global companies**

Since the early 1990s it has become clear that global companies (i.e., companies that conduct their business in many different countries) have become increasingly influential—sometimes even more influential than governments. As trade restrictions have been lifted (as a result of efforts by the World Trade Organization) and communications networks have become more sophisticated, multinational companies are now moving production and sales to wherever taxation and the supply of labor are most favorable.

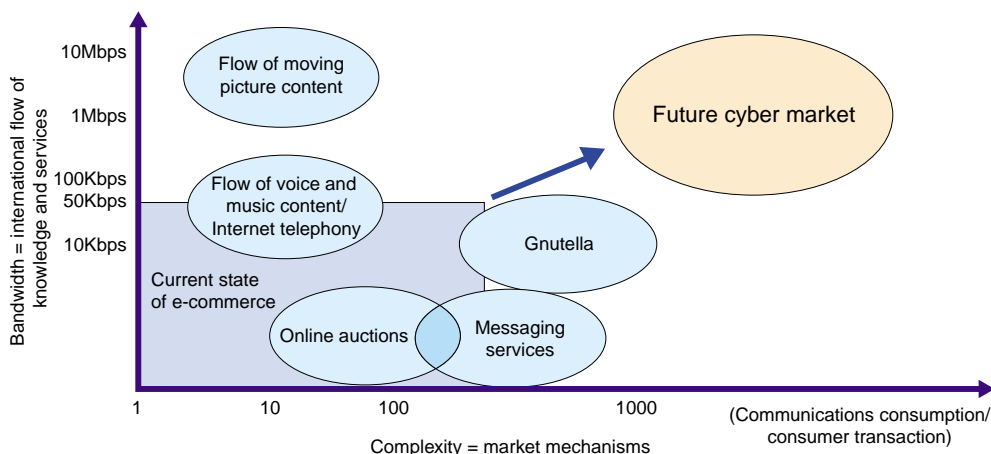
These global companies dislike national rules and have begun to demand that rules be unified as far as possible. In the field of e-commerce, these companies are playing an increasingly important role in helping to devise cyber rules. Another important development in recent years has been the growing influence of private citizens as information technology has become more a part of daily life.

**II Cyber Rule Systems**

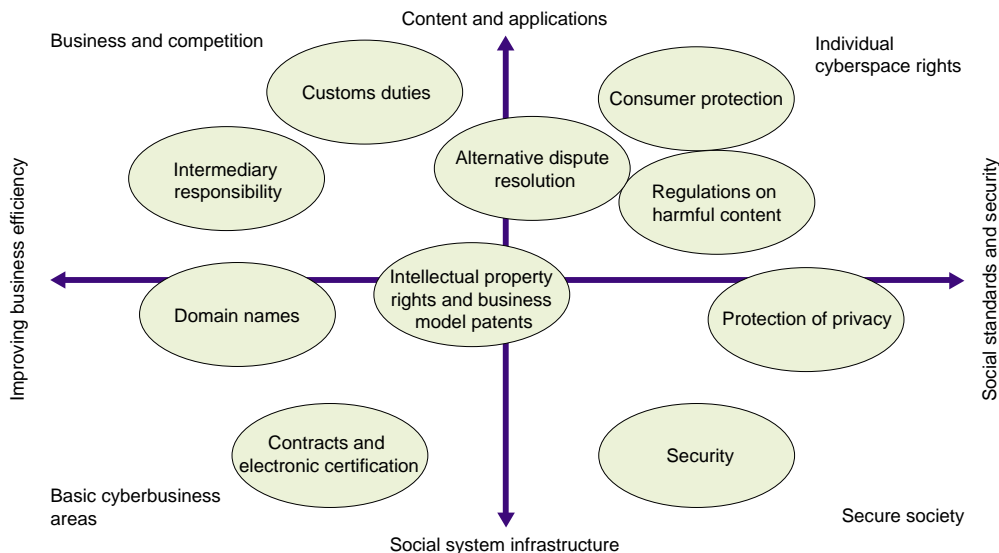
This section deals with cyber rule systems. There are two different types of cyber rules, and these can be plotted on two different axes. The first type (plotted on the vertical axis) deals with a matrix that shows whether the applicable rule supports the e-commerce infrastructure or covers content and applications. The other type (plotted on the horizontal axis) focuses on objectives and shows whether the rule aims at business efficiency or maintaining social standards and security. Figure 3 uses such a framework to categorize some of the issues concerning cyber rules that are currently the subject of debate.

Since 1995, the first area of cyber rules to become the subject of debate concerned matters of basic technology such as electronic certification. As e-commerce began to develop, the focus then shifted towards areas related to applications. Examples of the latter included such issues as how to protect intellectual property rights and

**Figure 2. Explosion in Bandwidth and Complexity**



**Figure 3. Different Types of Cyber Rules and Their Categorization**



the means to implement alternative dispute resolution (ADR).

One of the issues that are likely to arise in this basic area in the next few years is that of “convergence.” In this context, the term generally refers to the disappearance of the distinction between communications, broadcasting and the media. However, the emergence of ubiquitous networking (including the use of wireless communications and information appliances) is beginning to raise a wide range of related issues.

Examples of this would include access rules, resource allocation rules that would allow for universal service (i.e., essential telecommunications services provided at low cost to anyone requiring them) and international mobility (of services and handsets), and rules related to regulatory approval.

The area on the right-hand side of Figure 3 (social standards and security) shows how cyberspace—which was born and developed in an environment relatively free of restrictions—is now facing a large number of contentious issues, including the need to remove harmful content, as a result of the growing number of Internet users.

### III Structure of Rule Governance

This section deals with the question of who should be responsible for cyber rules and how they should be determined (i.e., the issue of rule governance). This is because an understanding of the structure of rule governance is an essential part of the vision needed to devise appropriate strategies. This issue is considered from four perspectives.

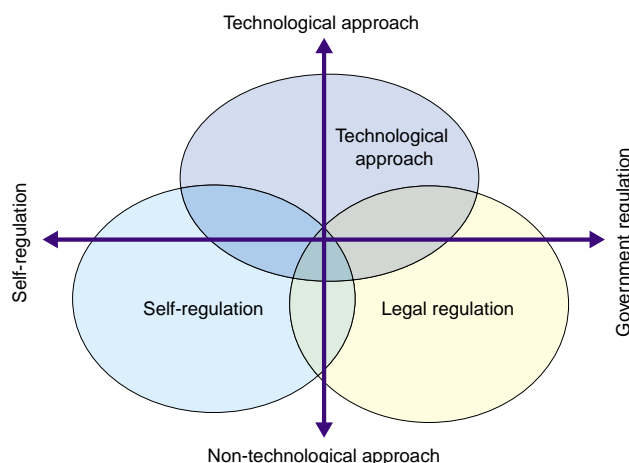
#### 1 Self-Regulation, Government Regulation and the Technological Approach

The Internet and its e-commerce offspring have developed mainly as a result of private-sector efforts. Accordingly, there is a consensus that the industry should be left to self-regulation as far as possible.

However, in matters such as the protection of privacy and the elimination of harmful content, self-regulation by the private sector is not enough. There is a growing belief that government regulation (including statutory restrictions) is also needed. It is probably fair to say that there is a constant tug-of-war between self-regulation and government regulation, with one or the other having the upper hand at any given time. Figure 4 represents such a governance model.

The figure allows for a third approach that is based on technology. This line of attack does not exclude the other two—rather, it is complementary. For instance, a new information distribution platform for protecting intellectual property rights would fall into this category. The debate about this technological approach is likely to be-

Figure 4. Three Approaches to Rule Governance



come increasingly heated in the next few years in the many areas where the debate about cyber rules is going on.

A technological approach inevitably means standardization and the emergence of a new global e-commerce platform. Such a cyber platform would have a global impact.

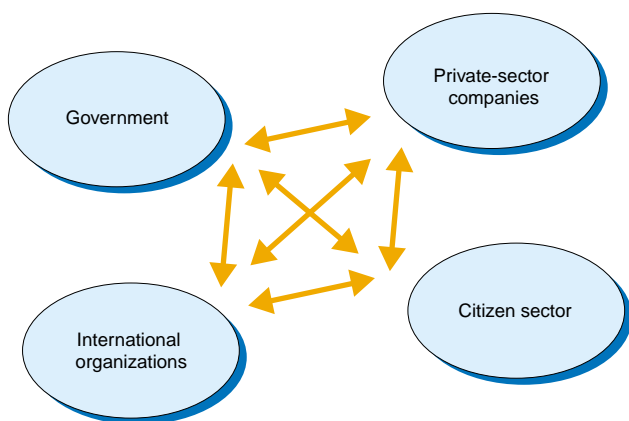
One example can be seen in the packages being marketed by leading computer vendors that are capable of performing complicated tax calculations for international e-commerce transactions carried out on the Internet. These packages have the potential to become global systems for levying and paying taxes. It is worth noting that powerful global companies and venture businesses are busy developing what they hope will be the cyber platform of the future.

#### 2 Role of the Private Sector, Government and International Organizations

The agreement reached on telecom deregulation at the World Trade Organization in 1997 marked the beginning of the international development of e-commerce. Some major private-sector companies interested in global e-commerce are making increasing efforts to play a part in devising global cyber rules. Figure 5 shows such private-sector companies alongside government, international organizations and the citizen sector.

The GBDe (Global Business Dialogue on Electronic Commerce) was founded in January 1999 with the participation of senior managers from leading European, African, North and South American, Japanese and Asian companies.<sup>3</sup> At its May 1999 conference that was attended by more than 300 representatives from national governments, international organizations and the media, a number of proposals were made that are designed to foster the development of e-commerce. At its general meeting in September 2000, the GBDe put forward proposals for cyber rules in each of nine different areas

**Figure 5. Those Involved in Rule Governance**



in its capacity as a private-sector business association. Its members include companies from developing countries, and it is endeavoring to expand its membership. At the same time, it is seeking to cooperate and enter into a dialogue with UN agencies and citizen organizations.

Other similar international organizations include the OECD’s Business and Industry Advisory Committee (BIAC), the Global Information Infrastructure Commission (GIIC) and the International Chamber of Commerce (ICC), while in the Asia-Pacific region there is the APEC Business Advisory Council (ABAC).

International organizations involved with cyber rules include the World Intellectual Property Organization (WIPO), UNCITRAL (see above), the International Telecommunication Union (ITU) and the International Court of Justice in The Hague. In order to keep up with developments in the rapidly changing field of e-commerce, these organizations are reorganizing and seeking to cooperate with the private sector.

Because private companies and groups exercise increasing influence in rule governance, there is a growing tendency for functions that have traditionally been performed by the public sector to be taken over by the private sector. For example, if disputes arise over rules, private-sector associations and venture businesses now offer alternative dispute resolution services that are working increasingly well. And functions that were formerly assumed to be the responsibility of the state are now being performed more efficiently by the private sector.

Another development in this field that will become increasingly important is international cooperation by the citizen sector. The appearance of non-profit organizations at the ministerial meeting of the World Trade Organization in Seattle in the autumn of 1999 is still fresh in the memories of many people, and companies can no longer ignore demands from consumer organizations for greater environmental protection and security. This role played by average citizens in rule governance is likely to become increasingly important. At its gen-

eral meeting in Miami in September 2000, for example, the GBDe began a dialogue with consumer groups about the issue of consumer credit.

### 3 Regional Models of Governance in the US, Europe, and Japan

In devising rules governing e-commerce, compatibility with domestic business practices should be carefully considered, as many regulations reflect national and regional cultures and are often unique. The following looks at regional approaches to cyber rule governance in the United States, Europe and Japan (see Table 1).

#### (1) Rule governance in the United States

The information technology industry has developed as a result of private-sector initiatives. Moreover, in the United States the Internet has developed in a spirit of self-governance as a private-sector business. The US dislike of regulation and belief in freedom and equality of opportunity are deeply ingrained in the information technology industry. As a result, there is a tendency for rules to be based on self-regulation. However, in some sectors more than others a need for government regulation is also felt, and the struggle between self-regulation and government regulation is likely to continue.

The US political system at the federal level consists of a legislative branch (Congress) and an executive branch (Administration), both of which are subject to considerable private-sector lobbying by companies trying to protect their interests. Similarly, staff on temporary leave from the private sector play an important part in the executive branch. In addition, there is an enormous market (based in Washington) of lobbyists and think-tank analysts who work on devising policy.

US companies are among the most competitive in the field of e-commerce and are advocates of global deregulation and the opening of service industries.

**Table 1. Regional Rule Governance Models**

Model	Characteristics
US model	<ul style="list-style-type: none"> <li>• Industry-led</li> <li>• Tendency to accept government regulation in areas such as the protection of privacy</li> </ul>
European/EU model	<ul style="list-style-type: none"> <li>• Rapid development towards regional integration by EU directives</li> <li>• Assertion of distinctive regional values such as privacy and security</li> </ul>
Japanese model	<ul style="list-style-type: none"> <li>• Government-led (less responsibility, slower pace of change)</li> <li>• IT Strategy Council, new developments such as discussions over a comprehensive bill to amend the existing onerous documentation requirements for all private-sector transactions</li> </ul>

## (2) Rule governance in Europe

In recent years, the EU has been more actively putting in place the systems needed to integrate e-commerce on a regional basis. As part of this, the eEUROPE initiative was launched by the European Commission.<sup>4</sup> The EU's efforts to maintain momentum by issuing directives and recommendations with a time limit are an indication of the seriousness with which it is trying to foster the development of e-commerce.<sup>5</sup>

One example of this is the EU's sudden change of policy on competition in the telecom industry. Similarly, the eEUROPE 2000 Action Plan, which was adopted in June 2000, calls for regional telephone networks to be opened by the end of fiscal 2000. This reflects the EU's acute concern that the US lead in this field may be increasing. Similarly, in areas such as the protection of privacy and billing for digital content, the EU has tried to emphasize the notions of security and fairness as a counterbalance to the American emphasis on market forces. Overall, the trend is towards liberalization and market development, but it is fair to say that the European model is distinct from that in the US.

The European Commission in Brussels has a staff of about 13,000 and is the place where the policies of most member countries are decided. Private-sector companies are apparently actively involved in this decision-making process, and their expertise is considered particularly important when deciding policy on e-commerce. This is reflected in the fact that groups of specialists based in Brussels are involved in policy creation via trade associations such as Electronic Commerce Europe (ECE), the Union of Industrial and Employers' Confederations of Europe (UNICE) and European Telecom Network Operators (ETNO).

## (3) Rule governance in Japan

At the risk of oversimplification, rule governance in Japan could be said to be dominated by the public sector. One of the advantages of this—for both society as a whole and for companies—has been that they have not been saddled with the responsibility of having to decide policy. This was fine when Japan was still in the process of catching up with the West and its industrial structure was changing relatively slowly.

In the age of e-commerce, however, when developments in information technology are led by the private sector and when rules and regulations have to change quickly (even at the risk of making mistakes) this has become a disadvantage. The problem is made worse by the fact that the pace of structural change in Japanese society is slowing and there is not enough energy to go after vested interests.

In terms of overall expertise in the field of e-commerce, Japan does not rank very high. However, the private sector has this year suddenly taken the lead as a sense of crisis has developed and organizations such as Keidanren (Federation of Economic Organizations) and the IT Strategy Council have made various pronouncements on e-commerce. A comprehensive bill that would amend the existing onerous requirements for documentation of all private-sector transactions is also under discussion.

## 4 Are Cyber Rules Going to Converge As a Single-Rule Model?

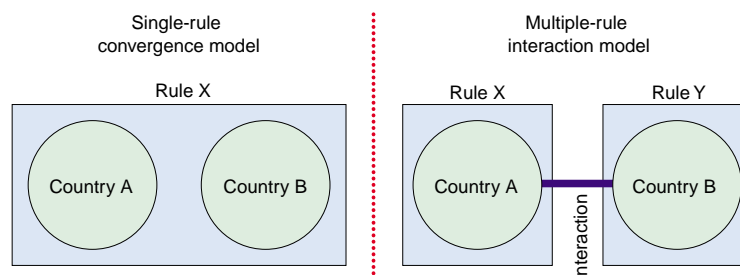
Global cyber rules can take one of two forms: they can either converge as a single-rule model or interact as a multiple-rule model. Figure 6 shows the two models. Because information technology thrives on economies of scale, it is possible to take the view that global cyber rules will converge on the US model. However, the recent developments in the EU suggest that it is also possible to come to see that global cyber rules will interact as in the multiple-rule model.

In general terms, the single-rule model would appear preferable in areas of basic e-commerce infrastructure and areas where business efficiency is sought (see Figure 3). Examples would be electronic certification and Internet domain names.

On the other hand, rules that allow for cultural and political differences seem more appropriate in areas that are closely linked to national interest—even when pursuing either social standards and security or business efficiency. Examples would be the issues of privacy and customs duties.

What balance should be struck between these two perspectives will depend on what kind of world we want

Figure 6. Cyber Rules: Convergence Model



and are likely to be the key questions in cyber rule governance.

## IV Issues Facing the Japanese Government and Japanese Companies

We have seen how the many companies, countries and international organizations that are competing to establish an e-commerce market are also engaged in drawing up rules for that market. With its technological prowess and the considerable benefits it has reaped from open economies, Japan has reached the stage where it needs to propose either a rule model of its own or an Asian model and to make a definite contribution.

Japan stands to derive considerable gains from ubiquitous networking (including information appliances). To develop this area, it needs to overcome not only technological but also institutional hurdles such as (1) how to produce rules for allocating wave frequencies to enable information appliances to communicate and (2) how to devise a system for distributing content. Let us look at the matter of allocating wave frequencies.

It seems reasonable to assume that, when many different information appliances are networked in the near future, they will be linked by high-frequency wireless connections. This means that ubiquitous networks are likely to depend mainly on domestic, office and public networks that are interconnected and independent of telecom operators. One system that could be used for this is the recently developed Bluetooth technology. This means that networking policy will shift from the “telecom operator model” to the “autonomous model” or the “vendor model.”

The problem is that today’s frequency allocation rules are based on the telecom operator model. At the moment, information appliances can use the 2.4 GHz frequency band, but this is too limited for high-frequency use. Consideration is therefore being given to using the 5 GHz band. In Japan, however, the issue remains unresolved because of the potential for frequency interference with the Meteorological Agency’s radar systems.

The issue of frequency allocation is complicated not only by the strict rules governing frequencies and field strength, but also the fact that licenses cannot be issued until an operator decides what type of wave system it is going to use. In a field such as this where companies are competing to develop new digital systems, this type of regulation has merely inhibited the development of new technologies and uses.

If Japanese electronics manufacturers are to develop and market new technologies for global application (and if the government is to support them), it would be more desirable if the Japanese government were to propose an international system for the use of radio waves. In fact,

however, the actual situation is just the opposite. In the case of the 5 GHz frequency band, for example, it was only after pressure from the United States and Europe that Japan considered allowing this frequency band to be used.

As long as Japan continues to follow the lead of others, it cannot expect to take the lead in areas such as ubiquitous networking (including information appliances). The international use of wireless and the convergence of telecommunications and broadcasting are likely to become an increasingly important field for cyber rules. Here Japan should take a leadership role rather than follow the lead of others.

Through its ODA program Japan is the world’s biggest donor of overseas aid. At the Okinawa Summit in July 2000, the Japanese government announced that over the next five years it would be giving \$15 billion in aid (mainly for Asia-Pacific countries) for both IT-related and non-IT-related projects. This is also the aim of Japan’s eAsia program. However, the most urgent need at the moment is for Japan to reform its own system in order to become a fully developed IT economy. To do this, it will need to devise a new process for deciding the policies that determine its posture in selecting and formulating the relevant rules.

In places such as Washington and Brussels, the networks and processes that determine policies are decided by people who understand technology, institutions and business. What Japan lacks is a market of comparable depth for determining policies. Those involved in the policy-making process—whether it be business people, the government, politicians or academics—need to be more involved at various levels, and there is an urgent need for political and administrative reform to make these systems more flexible.

Many US companies employ specialists and go to considerable lengths to have a say in how rules are devised. A move from public-sector control to private-sector initiative can only be successful if the private sector is willing to accept a heavy burden of responsibility. Companies will probably come to see that having staff who can exert influence on how such rules are devised internationally by private-sector organizations is an important element of their ability to compete internationally. Policy think tanks also have an important role to play in this field.

- (1) AOL’s Instant Messaging Service is a well-known and popular service that enables users to exchange long email messages (including conversation) in real time—something that is not possible with conventional email software.
- (2) An Internet identifier. For example, NRI’s domain name is nri.co.jp (compare its Web site address: <http://www.nri.co.jp>), and this is assigned to a particular address (or “IP address”).
- (3) Japanese companies participating in GBDe (“Global Business Dialogue on Electronic Commerce”) in-

clude Fujitsu, Hitachi, NEC, Toshiba, NTT, Mitsui Corporation, Sharp, NRI, MEI and Tokyo-Mitsubishi Bank.

- (4) Concerned that Europe was falling behind the United States in digital technology (including the Internet), the EU announced its eEUROPE Plan in December 1999 in the hope of making up the ground it had lost. This then served as the basis for the eEUROPE Action Plan 2002 drawn up by the European Commission and approved by the Council of Ministers at its June 2000 meeting in Portugal.
- (5) Under EU law, there are four different types of EU rules: (1) regulations (which, taken as a whole, are legally binding and must be adopted by all member nations), (2) directives (which are legally binding only with respect to their objectives but not in terms of their manner of implementation, which is left to individual countries), (3) decisions (which are legally binding in full only on those to whom they apply), and (4) recommendations (which are not legally binding).
- 
- (1) Takeshi Shinohara, “*Ninsho Gijutsu to Ninsho Bijinesu*” [Certification Technology and the Certification Business], *CHITEKI SHISAN SOZO* [Intellectual Asset Creation], Spring 1997.
- (2) Kiyokazu Yamakami, “*Denshi Shotorihiki Jidai no Hoseido*” [Legal Systems in the E-Commerce Age], *Joho Tsushin Autorukku '99* [IT Outlook for 1999], NTT Shuppan, 1999.
- (3) Takehiro Shinmori “*Beikoku ni Okeru Denshi Shotorihikiho no Kento Jokyo*” [E-Commerce Legislation in the United States], NBL, April, May and July 1999.
- (4) *Denshi Shotorihiki no Kankyo Seibi no Ikkann to Shite no Hoteki Kadai ni Tsuite* [The Legal Aspects of Laying the Foundations for E-Commerce], Ministry of International Trade and Industry, August 1999.
- (5) “The Digital Economy in International Perspective: Common Construction or Regional Rivalry,” A Conference of the University of California E-Conomy Project, May 27, 1999.
- (6) Isamu Sugishita (trans.), “*eEurope Akushon Puran*” [The eEUROPE Action Plan], *Kaigai Denki Tsushin* [Telecommunications Abroad], September 2000.
- (7) Catherine L. Mann, Sue E. Eckert and Sarah Cleeland Knight, *Global Electronic Commerce: A Policy Primer*, Institute for International Economics, 2000.
- (8) Association for the Study of Cyber Law (ed.), “*Saiba-supesuho*” [Cyber Space Law], Nihon Hyoronsha, 2000.
- (9) Hideyuki Okamoto, “*Joho Tsushin Bun'ya no Seisaku Kettei ni Okeru Rieki Shudan no Yakuwari*” [The Role of For-Profit Groups in Deciding Policy on Information Technology], *ITU Janaru* [ITU Journal], May-July 2000.
- (10) Seiichi Yoshikawa, “*Denshi Shotorihiki no Kazeijo no Mondaiten*” [Taxation Issues in E-Commerce], *Kokusai Zeisei Kenkyukai* [Association for the Study of International Taxation], No. 4. October 2000.
- (11) Tomoyuki Watanabe, “*Kurosubodatorihiki to Shohi Kazei—Denshi Shotorihiki e no Taio*” [Cross-border Transactions and Consumption Taxes: Dealing with E-Commerce], Hitotsubashi University Economic Research Institute discussion paper, March 2000.
- 

**Takeshi SHINOHARA** is a senior consultant at NRI's Center for Knowledge Exchange and Creation. He is also a visiting professor at Osaka University and the Kyoto University Graduate School as well as a part-time lecturer at the Tokyo Institute of Technology. He specializes in information and communications technology policy.

As a leading think-tank and systems integrator in Japan, Nomura Research Institute is opening new perspectives for the 21st Century through creating intellectual property for the benefit of all industries. NRI serves domestic as well as overseas clients both in the public and private sectors through knowledge creation and integration in the three creative spheres of “Research and Consulting,” “Knowledge Solutions” and “Systems Solutions.”

With the opening of the new millennium, the world economy is facing rapid structural changes led by the dramatic growth of IT industries and the rapid expansion of worldwide Internet users—the challenges of which require new concepts and liberation from outdated systems. As one of Japan’s top solutions providers, NRI is dedicated to equipping its clients with strategies for success in this difficult environment through providing the best in knowledge resources and solutions.

*NRI Papers* presents selected works of NRI’s 3,000 professionals in its worldwide research network. The mission of *NRI Papers* is to contribute new ideas and insights to business management and future policy planning that are needed to overcome many of the obstacles before us.

All copyrights to *NRI Papers* are reserved by NRI. No part of this publication may be reproduced in any form without the prior written consent of NRI.

Inquiries to: Editorial Section I  
Corporate Communications Department  
Nomura Research Institute, Ltd.  
E-mail: [nri-papers@nri.co.jp](mailto:nri-papers@nri.co.jp)  
FAX: +81-3-5255-9373