5

Digital Content Distribution and Copyright Manegement Technology in the Broadband Age

TETSUYA YAMAZAKI
Information and Communications Research Unit

5.1 Introduction

Development of digital technology and the sophistication and rapid spread of personal computers have resulted in digitization of a variety of content such as software, documents, photographs, paintings, music and video, which is now widely distributed over networks like the Internet. In addition, the emergence of broadband access lines to the Internet, typically ADSL, is enabling transmission of digital content via networks in significantly larger volumes and higher quality than through the conventional technologies. In particular, distribution of entertainment content such as music, movies and TV dramas, which plays an essential role in promoting the use of broadband networks, is expected to form a major market in the business to consumer (B2C) segment. Other areas having large potential include new services combining digital broadcasting with network communications, and the new hardware devices to support such services.

On the other hand, as digital content is known to be easily copied and distributed online while minimizing degradation from the original during copying, illegal replication and piracy have been causing critical problems. Now that a large number of illegal copies are available on the Internet, the situation is becoming more serious.

In order to expand the legitimate digital content market online, copyright protection technologies to prevent the creation and distribution of such illegal copies are indispensable. At the same time, laws and social systems that are suited for copyrights in the broadband age will soon be demanded.

This report focuses on copyright protection technologies for entertainment content (books, music, movies, etc.) in the B2C segment with additional consideration on developments concerning the copyright law. Note that copyright in general consists of copyright in a narrow sense and neighboring rights: the former is given to the creator of music, a novel and so on while the latter is given to adapters of works over their musical arrangement, scriptwriting, editing, etc., as well as to performers such as musicians and actors and to producers of sound recordings, movies and so on. Whereas more detailed definitions exist, this report only covers copyright in a broad manner, which includes both copyright and neighboring rights.

5.2 The current status of digital content distribution

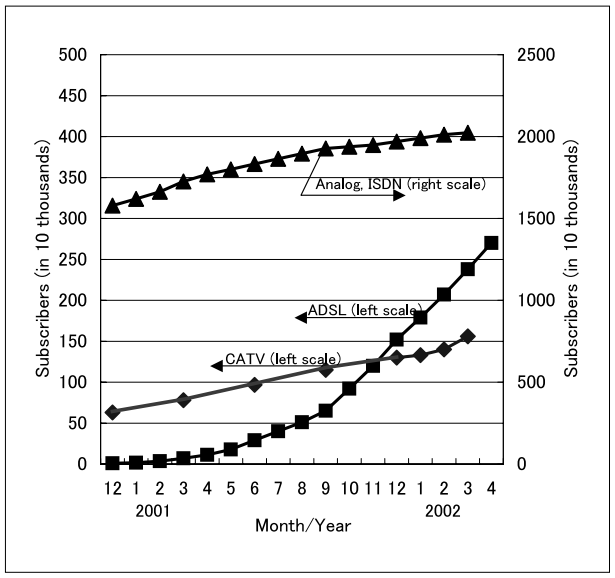
5.2.1 Spreading broadband and its capability

Among the available broadband connection services, through which users are allowed faster communications than ISDN (64 Kbps/128 Kbps), CATV Internet and ADSL (around several Mbps) have been sharply increasing the number of their subscribers since the middle of 2001 (Figure 1).

On the other hand, the number of subscribers of optical fiber connections, a service that utilizes fiber-optic networks to provide more than a 10 Mbps transmission speed, remains relatively small at 26,000 (preliminary chart from the Ministry of Public Management, Home Affairs, Posts and Telecommunications) as of the end of March 2002, probably because of the limited areas of coverage. However, the chart is expected to grow rapidly as the coverage areas expand in the future.

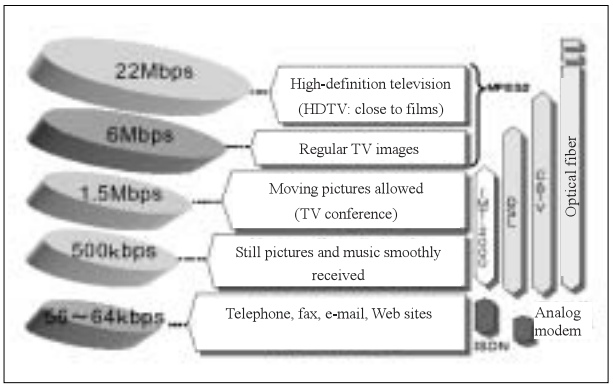
The currently popular ADSL and CATV Internet

Figure 1: Number of Internet connection service subscribers



Source: Ministry of Public Management, Home Affairs, Posts and Telecommunications, "Prompt report on the number of Internet connection service subscribers as of the end of May 2002."

Figure 2: Transmission speeds and distributable content



Source: Study Group of the Ministry of Public Management, Home Affairs, Posts and Telecommunications, "Toward copyright protection of digital content and smoother network distribution."

connections offer transmission speeds ranging from hundreds of Kbps to several Mbps, and are enabled to distribute near-TV quality moving images when combined with image compression technology. If optical fiber communications, which are even faster, become widely available, distributing moving pictures comparable to those on high definition TV (HDTV) will become possible (Figure 2).

In response to such developments, Internet service providers (ISP) and content holders (creators and owners of content such as movie companies, TV networks and record firms) have already begun services to distribute digitized music, images, books, and so forth (Table 1). Some are finding niches by offering exclusive content such as several-minute short dramas, Korean movies, and interactive material specifically created for broadband.

Material like movies, music and software have long been considered suitable for online transactions, because a transaction can be completed without physical transportation of the goods if payment and data exchanges are made over networks. Even a traditional hurdle that data exchanges via slow connections like analog modems and ISDN take too long is being overcome by the spread of ADSL.

Of the entire B2C e-commerce market in Japan, which was worth ¥1,484 billion in 2001, the digital content market accounted for approximately 6%, or ¥93 billion. However, as much as ¥86 billion of this (about 90% of the digital content market) was from mobile telephone (sales of ring melodies, idle screen images, etc.), indicating that the market targeting broadband has just begun to bud (by "FY2001 survey of e-commerce market scale and conditions," Ministry of Economy, Trade and Industry).

Table 1: Content distribution services

Category	Service Name (provider)	Distributed Content
ISP	Yahoo! BB (Yahoo! BB)	Moving images, games, books, etc.
	Nifty (Nifty)	Short films, games, music, etc.
	Dream Screen (DTI)	Movies, film previews
Content holder	TV-Tokyo Broadband, etc. (TV stations)	Previews, behind-the-scenes video, short dramas, TV programs
	Label Gate (Sony)	Music
	@music (AVEX)	Music
	Chuokoron-Shinsha	Electronic books

Source: Author's compilation from newspaper articles and other data.

5.2.2 Actual conditions of illegally used digital content

Digital content is:

— Easy to copy (mass and quick replication is easier than analog content).
— Easy to distribute online by using compression technologies.
— Not degraded by copying.

For such characteristics, illegal copying and piracy have been major problems for digital content. The situation is worsening now that an enormous number of illegal copies are available over the Internet. Once an illegal copy is posted online, it can instantly spread throughout the world. In the case of musical works, illegal copying is extremely rampant, since most of the CDs are not copy-protected, data extraction and compression from CDs are easy on PCs, and compression technologies like MP3 have become commonly known. Even large-volume content such as software and motion pictures has begun to suffer from the same trouble as broadband users grow. Furthermore, the emergence of peer-to-peer (P2P) file exchange technology accelerated illegitimate copy distribution.

With P2P technology, which is attracting attention as a next-generation Internet tool, users can share or download files (data) stored on other computers over the network. It has advantages such as allowing data to be shared through the Internet without a particular server constantly connected online and permitting users to search for and retrieve information without a search functioning server. By using Napster, Gnutella, WinMX or other free programs, users can easily post and trade over the Internet music data created by copying CDs they personally own.

In the U.S., the Recording Industry Association of America (RIAA) and others filed lawsuits against Napster and other P2P service providers, demanding them to pay copyright fees and to eliminate unauthorized copies from their servers. Also in Japan, MMO Japan Ltd., a company that had started a Napster-like service, was ordered by the court to stop service in a case brought by record companies and others. Whereas it is not clearly known how many illegal copies are distributed online, RIAA stated in court that 300,000 accesses were being made to Napster's Web site per day. Another survey by the Association of Copyright for Computer Software (ACCS) and the Recording Industry Association of Japan (RIAJ) estimates that the total number of downloaded music files through P2P services up to January 2002 reached 75 million in Japan.

It should be recognized, however, that there is nothing illegal about the P2P service itself, and, furthermore, it is given a lot of attention as a useful technology. Should the illegal copy issue lead legislators to regulate it, development of the Internet would be adversely affected. On the other hand, posting illegal copies of copyrighted material is regulated by World Intellectual Property Organization (WIPO) treaties as mentioned later and thus illegal in countries like Japan that have enacted laws in accordance with the treaties.

5.3 Copyright management technology

5.3.1 Digital rights management (DRM) system

In the similar way the criminal law cannot stop a burglar from breaking into an unlocked house, the copyright law cannot protect copyrights without copyright protection technology, which acts as a lock for copyrights. The mainstream of traditional copyright protection technologies has been the copy protection applicable to home recording devices (Table 2). In addition to this, however, digital content distribution in the broadband age requires data at any stage of its process — from transmission over the network to end user's playback and copying to storage media — to be prevented from exposure, because once the data is exposed and recorded, it can be easily replicated and distributed online. In addition, measures against cracked protection and distribution of illegal copies are needed. To this end, a comprehensive protection system that covers a variety of entities — from distributors, user terminals and output devices to storage media — needs to be established. The scheme is called the Digital Rights Management (DRM) system (Figure

3). All protection technologies, including conventional ones, that are used for DRM and related systems are collectively referred to as copyright management technology in this report.

Table 3 shows major DRM technologies. Some of these technologies require special hardware such as a memory card, while others ask users to obtain a separate license for each memory card they use because of the lack of compatibility between networks and user terminals. With respect to output to digital displays, standardization of the authentication and encryption methods between connectors is in progress to define the specifications of output connectors (USB and IEEE1394) used apart from DRM.

5.3.2 Measures against cracked DRM

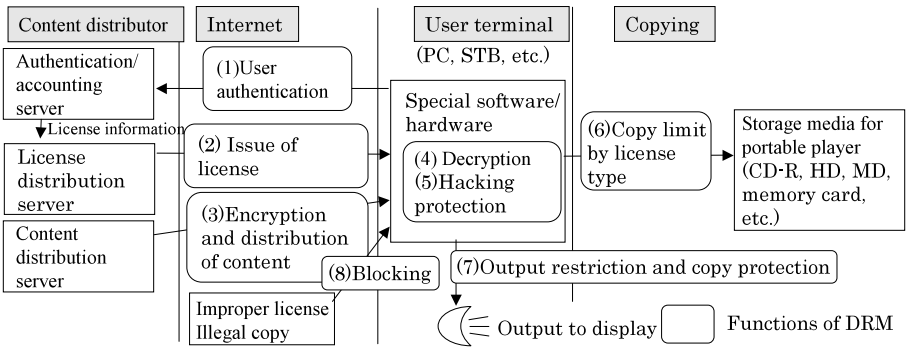
However tough a DRM system is, there is always

Table 2 : Major conventional copy protection technologies

Name	Applied Media	Outline	Standardization Body
Macrovision	VHS videotape, DVD	Copies are identified through signals added to analog video data, and their images are scrambled when played.	Macrovision (U.S.)
SCMS (Serial Copy Management System)	MD, DAT, CD-RAM, DVD, etc.	Permits only first-generation digital-to-digital copies of music.	Sony, etc.
CSS (Content Scrambling System)	DVD-Video	Encrypts content to disable direct copying of digital data.	DVD Copy Control Association
CPPM (Content Protection for Prerecorded Media)	DVD-Audio	An enhanced mechanism of CSS.	Same as above
CDS	CCCD (Copy Control CD)	Partly changes the file data to prevent ripping (taking out music data) on PCs. The media is playable on regular CD players.	Midbar-Tech (U.S.)

Source: Author's compilation from "Home Network" (Atsushi Matsushita et al., Shokabo) and others

Figure 3: Digital right management system



(1) During user authentication, software/hardware is checked for conformity to the DRM.
(2) License includes the encryption key and conditions to use the content (playable period/times, copy limit, etc.). To prevent the illegitimate use of the license, an encryption key is used, for example, in combination with a unique ID of the special software/hardware.
(3) When encrypting the content, content ID, terms of use and electronic authentication data (for preventing forgery of IDs and terms of use) are sometimes encrypted together with the content itself. This is called encapsulation. Aside from distribution via networks, distribution in the form of CD-ROMs or other media should also be taken into account.
(4) Access from the outside to the decrypted content is blocked.
(5) To prevent the content and encryption key from leaking out by the cracking of software/hardware, encryption of software or other measures are taken.
(6) Whether the copy destination is conformable to the DRM is verified and the total number of copies is controlled. Also, further distribution of copies is prevented through measures such as encryption by using the unique ID of the copy destination.
(7) For digital output, the destination is authenticated and the data is encrypted between connectors. For analog output, copy protection technology like Macrovision is sometimes used.
(8) Illegal copies, which are detected by digital watermarks, etc., are barred from use. Information about illegitimate licenses and cracked encryption keys is distributed, so as to invalidate them or to deliver new encryption keys.

Source: Author's compilation from the homepage of Recording Industry Association of Japan, etc.

Table 3: Major DRM technologies

Company Name (technology name)	Outline
Microsoft (WMRM, Windows Media Rights Manager)	Part of Windows Media Technology (WMT). To play content, a license that contains a decryption key and terms of use is needed separate from the content. The license cannot be copied to another terminal to play the content.
InterTrust (MetaTrust Utility)	A U.S.-based venture business. Adopted by Real Networks. Information on access control and accounts is encrypted/distributed with content. For each use, access terms are checked and charging data is sent for processing at the central office.
IBM (EMMS: Electronic Media Management System)	Consists of five software applications including a content mastering program, a hosting tool to store/distribute content in EMMS format ??and a sales system to supporting online stores.??
Sony (Open MG/Magic gate)	A copyright protection technology developed by Sony. It works with MDs and memory sticks. Compatible with IBM's EMMS technology.
Fujitsu, Hitachi et al. (UDAC: Universal Distribution with Access Control)	Supports the superdistribution scheme (separate distribution of content and license). Applied to solutions designed for PCs. Uses the Secure Multimedia Card (MMC) as the storage medium.
Intel, IBM, Matsushita, Toshiba (CPRM: Content Protection for Recordable Media)	A copyright protection technology that can be built into hardware devices such as hard disks and memory cards. Used for the SD memory card system called "SDAIR."

Source: Author's compilation from a report by the Study Group on the Formation of the Network Distribution Market of Digital Content of the Ministry of Public Management, Home Affairs, Posts and Telecommunications, and Web sites of relevant organizations.

a risk of it being cracked. In addition, a 100% secured DRM technology would cost too much and provide less usability for both users and content distributors.To be more realistic, measures to minimize damage in case of cracking should be incorporated into DRM, with its primary goal set as prohibiting non-expert users from effortlessly making illegal copies (so-called casual copies). If a DRM technology is broken and the protected content illegally leaks out onto networks, the following measures should be taken.

(1) Detect the illegal content on the network.
(2) Filter and block the illegal content on the server side.
(3) Filter and block the illegal content on the user side.
(4) Track down the location of the leak.
(5) Suspend and update the key/license.

Step (1), which is usually carried out by a program that automatically makes the rounds of the network, is not effective if the original file names and extensions are changed. In step (2), the files detected during step (1) are screened and blocked on the servers of the ISP, which also fails to detect files with their names changed. For step (3), a certain control code or ID should be embedded in the content in advance so that it can be identified. Step (4) requires the ID of the legitimate user or playback system to be embedded in the key or the content itself.

The most preferable method is to embed a preset ID or control code in the content, and detect and block it based on that signal. If the user information is included in the ID, the location of a leak can be easily discovered. To inhibit the removal of the embedded ID in the content, digital watermark technology, which is mentioned later, is used.

In step (5), a list to invalidate the leaked content and the relevant keys is issued, the keys are renewed, and the access right of the user (system) who is responsible for the leak is suspended. The updated invalidation list also needs to be transmitted to user terminals. This process should preferably be conducted automatically. As of this point, no DRM system is known to be capable of carrying out the complete set of these measures.

While DRM technologies that use specifically designed hardware such as mobile telephones or set-top boxes (STBs) are, in general, harder to break, they require extra costs and penetration of such devices. Difficulty with improvements and upgrades of devices in the case of cracking is another disadvantage of hardware-oriented technologies. On the other hand, although DRM solutions that are based on software like computer

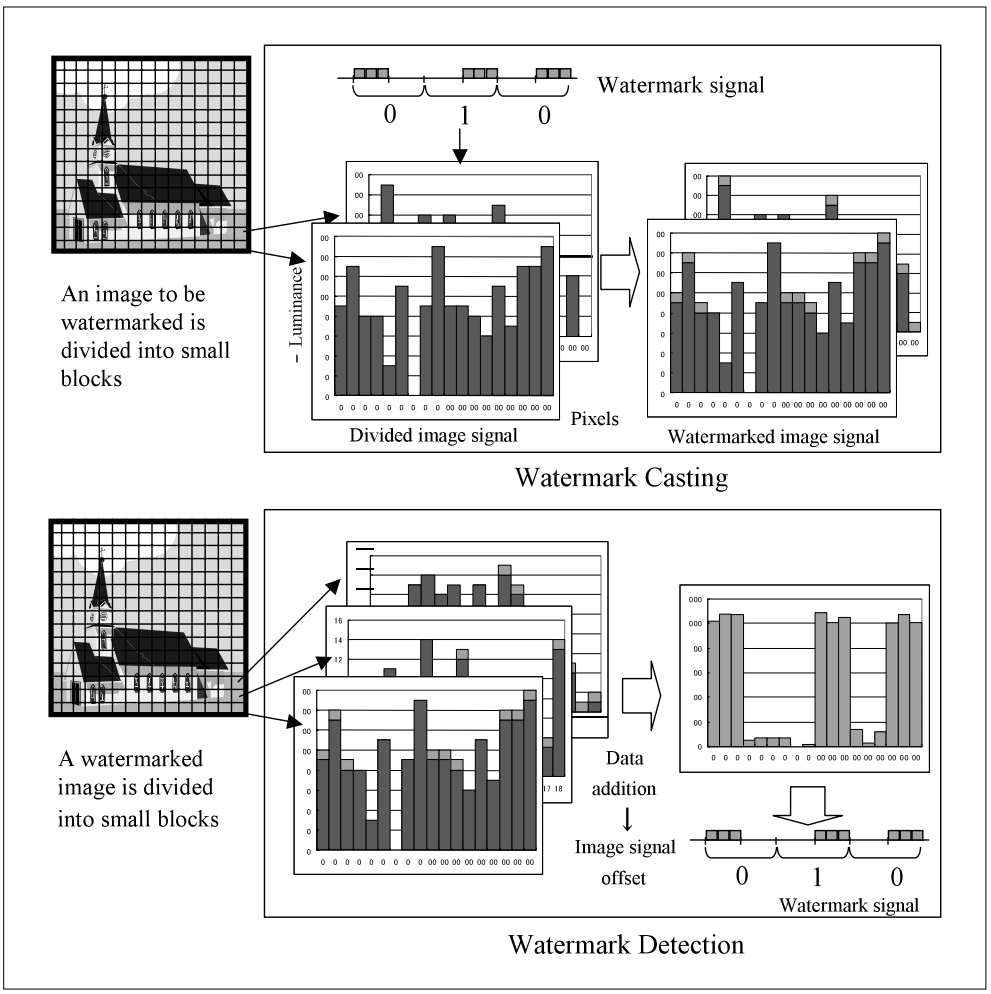
applications are relatively vulnerable, a countermeasure in the case of cracking can be as simple as distributing an upgraded version of the software over the Internet.

5.3.3 Digital watermarking technology

Digital watermarking technologies are used to place a non-removable signal on content. As mentioned before, signals such as copy control code, code to detect illegal copies, unique content IDs and user/author IDs can be embedded as effective measures against illegitimate copy distribution. There are two types of watermarks: invisible watermarks are imperceptible to human senses, and visible watermarks are used to indicate "sample" signs or to stamp the name of the author. Generally, invisible watermarks are employed for copyright protection.

Figure 4 shows how digital watermarks work. For invisible watermarking, the content signal is divided into small blocks of time or area, each of which a watermark signal is inserted into. A watermark signal is defined as, instead of the absolute value, relative information calculated by, for example, comparing two consecutive blocks to see which has a higher value. To decode the watermark, signals are synchronized with the division cycle, so that the original content signals add up to random signals to offset each other while watermark signals intensify each other so as to be detectable (there are many other schemes). Robust watermarks that can withstand image processing such as compression, scaling and cutting while imperceptible during legitimate use are needed. To meet these two conflicting requirements, watermark developers are building a variety of mechanisms to insert or adjust the signal — for example, a scheme in which a strong signal is embedded to highly detailed areas and a weak signal to flat areas. Despite their efforts, none of the current digital watermarking systems resist well to distortions like random bending

Figure 4: How digital watermarks work



Source: Author's compilation from materials made by Hitachi, Ltd

attack, in which random parts of an image are distorted. The volume of an inserted signal is typically several hundred bytes.

While there are many problems to be resolved, including cost issues and standardization (a requirement for application to packaged products like DVDs), watermarking is an effective technology to prevent distribution of unauthorized copies and, thus, its early commercialization is awaited. Also needed are systems to confirm the distributors of illegal copies in a manner they cannot repudiate such violation, for instance, by combining the digital watermark with a digital signature or allowing authentication by a third-party organization.

5.3.4 Standardization of DRM

For the benefit of users as well as content providers, a universal standard or compatibility should be provided for DRM. In practice, there are a variety of DRMs designed for different types of content or platforms. As shown in Table 2, several DRM technologies are competing to become the de facto standard for PC-oriented platforms. As a preparation to the rise of home networks (networks built within homes by using home servers, which are divided into audiovisual-oriented and white-goods-oriented), some vendors of PC-based DRM systems are promoting their technology for adoption to other distribution channels while others are enhancing their systems' compatibility with different types of content and distribution channels.

In the area of audio content, the Secure Digital Music Initiative (SDMI) led by RIAA had been consolidating the specifications for music distribution over the Internet and for recording/playback devices. In 1999, SDMI released Phase 1 specifications, which demand restriction on the number of copies and the adoption of digital watermarks. Many of today's DRMs are compliant with Phase 1. Next, SDMI began discussing Phase 2 to specify how to detect illegally copied music from digital watermarks and to prohibit its playback, only to fail in reaching an agreement and dissolving in 2001. However, the specifications set by SDMI are expected to remain effective in the industry as a standard required by copyright holders. In Japan, the Japanese Society for Rights of Authors, Composers and Publishers (JASRAC) has been selecting recommended digital watermark technologies for music under projects called Step2000 in 2000 and Step2001 in 2001.

In the motion picture field, the Copy Protection Technical Working Group (CPTWG), an organization where international standardization of copy control technology is discussed among content providers, IT companies and home electrical products manufacturers, and the DVD Copy Control Association (DVD CCA), a standardization body for DVD copy control technology, are working on standards for copy protection and encryption, while the Video Watermark Group, a joint organization of CPTWG and DVD CCA, is specifying the requirements for digital watermarks.

5.3.5 Content ID

An obstacle to content distribution over networks, aside from the ones arising from copyright management technology, is the complication of the copyright authorization procedure. This is especially true for content such as a TV program, where many copyrights (and neighboring rights) are involved and there is no standard procedure for handling copyright agreements. In such a case, a process of obtaining additional permissions from all copyright owners for distribution over networks could be an extremely difficult task. To make matters worse in Japan, copyright holders often grant authorizations without written contracts, or if any, conditions on the scope of permitted rights are most likely left unclear, further inhibiting content commerce. Another challenge is that copyright holders sometimes want some of their works to be used under certain conditions (with the indication of the author's name, with no modification without permission from the author, etc.) rather than protecting them with DRM. However, defining terms of use for individual copyright properties would be troublesome for copyright owners and time- and cost-consuming for content users, who would have to contact the owner to confirm the terms before distribution.

As a solution to this, the mechanism of "Content ID" is under development as a means to identify digital content with a unique code that is assigned

to each content item in accordance with a database containing the copyright holders' information and licensing conditions. Content IDs are embedded into digital content by using digital watermarking and other technologies. Groups working toward this goal include the Content ID Forum (cIDf), established by Prof. Yasuda at the University of Tokyo and involving Matsushita, Hitachi, NTT and other companies, ISO/MPEG21 (Moving Picture Experts Group 21) and ISO/TC 46 (Technical Committee 46, which is developing an identification system for movies). The Content ID scheme studied in cIDf, for example, offers DRM functions such as copy protection and encryption of content data, other than the capacity of identification.

On a national level, the Ministry of Economy, Trade and Industry and the Ministry of Education, Culture, Sports, Science and Technology (the Agency for Cultural Affairs) take the initiative in similar activities. They are building a database system called the Japan Copyright Information Service (J-CIS) as a model for centralized management of copyright information, although there are many problems to be solved such as who will be in charge of database management and who will bear the expenses.

5.3.6 *New forms of content and copyright distribution*

In conventional content distribution, content would be sold through distributors (publishers, music labels and broadcasting companies) under contracts with the author, who would later receive the profits. The spread of the Internet and broadband connectivity services have raised the possibility of a new type of content distribution in which the author can directly sell his or her works to the general public. Many software programs, mostly those developed by individuals, are now distributed as shareware, for which a user pays directly to the author, and freeware, software that is available without charge but sometimes with restrictions on use and redistribution. Even musical works and novels are sometimes seen sold on their authors' web sites.

Such distribution by authors, however, puts both the author and the user through much trouble with payment transactions, license (a key for the user to decode encryption) management and other procedures. To save them from having to carry out these complicated tasks, web sites such as Vector (Vector Inc., the operator of a shareware download site) have emerged to provide online marketplaces where license management and license-fee collection for digital content created by individuals are carried out by the site operators.

Another new approach to content distribution is superdistribution, a concept in which digital content is made available freely so that content providers can automatically charge a small fee for each use of their content, proposed by Dr. Mori, emeritus professor at the University of Tsukuba. Widespread availability of constant connection services has made the costs for transmitting accounting information, which is an essential element of superdistribution, negligible and has led to the development of a compatible DRM system. This new form of content distribution, however, has yet to be disseminated widely. Taking a view opposite to superdistribution, a service in which a user who purchases a license is allowed access to the content stored on the server from anywhere on the network has launched on a limited basis.

Just like content, copyrights may be distributed through direct transactions between the author and the user or through an intermediary. Copyrights for illustrated images, photographs and music to be used on personal web sites could be sold in the form of licenses for the right of public transmission. Such distribution may also provide content distributors with the possibility of uncovering prominent amateur works.

What are required in order for these new distribution systems to spread are an inexpensive settlement system to handle small payments, reliable copyright management technology available at low prices, a standardized copyright contract that is simple as well as easy to understand, and a copyright information management mechanism like Content ID.

5.4 Developments in relevant legislations

To reflect copyright holders' urgent demand for a new form of copyright protection to cope with

digitization and networking, in December 1996, the World Intellectual Property Organization (WIPO) adopted two treaties: the WIPO Copyright Treaty (provisions about software copyright, prohibition of the circumvention of copy protection systems, the right to transmit copyrighted works like phonograms through networks, etc.) and the WIPO Performances and Phonograms Treaty (provisions about the rights given to performers to transmit their works through networks, etc.). With respect to content distributed over networks, these treaties have granted copyright holders the right to make public transmission of copyright works (right of public transmission) and the right of holding such works in a transmittable state, as its previous step, on a server or other storage media (right of making transmittable).

In Japan, where the right of public transmission has already been incorporated into the Copyright Law in 1986 to cope with online karaoke systems, the government amended the Copyright Law as shown in Table 4 in line with these treaties. As a result, the right of making transmittable was given to broadcasting and cable broadcasting companies, making the Japanese Copyright Law more sophisticated than its counterparts in many other nations in terms of content distribution.

On the other hand, in the U.S., the Digital Millennium Copyright Act was enacted in 1998 to regulate the circumvention of copy protection systems and to define the procedure to remove illegal copies from networks (notice and takedown). However, this law does not cover the right of making transmittable. Therefore, the Napster case was prolonged, disputing whether exchanging copies of copyrighted materials stored on individual users' computers via P2P falls within the scope of the social agreement about the use of personal copies, or "Fair Use," and whether Napster aids and abets infringement of copyrights through its services. Japan also has provided a procedure similar to notice and takedown in the "Law Concerning the Limitation of Damages to a Specific Telecommunications Service Provider and Disclosure of Sender Information" issued on November 11, 2001.

Meanwhile, China, where the Business Software Alliance (BSA) and others point out that piracy is commonplace, revised its copyright law in October 2001, as it became a full member of WTO. The amendment prescribes for copyrights in a networked environment, which are equivalent to rights of public transmission and making transmittable in Japan, legal procedures to help victims who are seeking court orders to stop violations and to seize evidence, and for compensation from overseas entities (Copyright

Table 4: Amendments to the copyright law of Japan concerning digital content

Revision in 1997	— Wired/wireless interactive transmission was defined as "automatic public transmission" and the overall transmission including this was defined as "public transmission." Right to make public transmission of copyright works was given to copyright holders. Right of public transmission includes the right of making transmittable as its previous step, under which works are held in a transmittable state. — Right of making transmittable was newly given to performers and phonogram producers.
Revision in 1999	— Manufacture and distribution of devices intended to circumvent copy protection and other technologies to protect copyrights were restricted. — Illegitimate modification or removal of copyright control information was restricted. — Rights of distribution and presentation, which had been only associated with films, were expanded to other copyright material.
Revision in 2000	— Cases in which works can be used for the vision or hearing impaired without permission of the authors were specified. — Provisions on judicial procedures against copyright infringements were enhanced and the ceiling of a fine was raised from ¥3 million to ¥100 million to further deter violations.
Revision in 2002	— Right of making transmittable was given to broadcasting and cable broadcasting companies.

Source: Author's compilation from data on the Web sites of the Copyright Research and Information Center, the Cultural Affairs Agency and others.

Research and Information Center, People's Daily/Nikkei Biz-Tech).

Since the Internet can deliver information across national boundaries, illegal copying may not be controlled solely by civil laws. In fact, some P2P companies are leaving Western nations to escape from their strict regulations and intend to continue their business in third world countries. Copyright policies differing from state to state and lobby groups with strong political influence like RIAA also contribute to the current lack of international cooperation in legislation for copyright protection. In fact, the signatories of the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty barely reached 34 and 30, respectively, as of March 2002 (data from Copyright Research and Information Center). Meanwhile, Japan, which had not joined the WIPO Performances and Phonograms Treaty, made a decision on accession to the treaty in June 2002.

5.5 Conclusion

Some copyright protection technologies such as DRM have already been put to practical use, allowing music and other content distribution services to launch. As mentioned in chapter 5.3, however, the lack of compatibility between DRM systems or between hardware devices can make such schemes unfriendly to users. Considering the difficulty with standardization under the fierce competition among DRM vendors, other means to enhance compatibility are called for.

Conventional content distribution systems relied on technologies in which data is transmitted in a form inseparable from "physical" entities such as books, CDs and DVDs, or in which data is broadcasted under centralized control. The widespread use of tape recorders and VCRs enabled content to be treated independent of physical products, and freed it from constraints such as timetables and show schedules. The emergence of broadband networks, digital broadcasting and other new distribution channels, and the penetration of PCs and other networked appliances to record/play digital content are bringing about an environment in which content can be distributed as information. When the third-generation mobile telephone and high-speed wireless LANs become more prevalent and the capability of mobile digital devices further enhances, people will be able to use any desired content anywhere, any time. In reality, however, many of the current DRM systems intend to protect copyrights by linking the content with physical entities (specifically-designed devices and storage media) to meet the demands of content holders. This is where they are failing to cater to users, as indicated before. There are other technical attempts that have yet to come into wide use. One of them is DRM based on superdistribution, a concept in which content is distributed freely and content providers can automatically collect payments for the use of their services.

Widespread use of PCs and personal recording devices has enabled individuals to create digital content with ease. Furthermore, taking advantage of increased connectivity to the Internet, anybody can post his or her works to the general public throughout the world. From this perspective, copyright management is no longer an issue only concerning specific copyright holders such as professional writers, composers, and movie and record companies. A copyright protection technology that can provide a balance between user-friendliness and protection ability, while securing availability to anyone, is being awaited for to come into common use.

Acknowledgements

I gratefully offer my thanks to Mr. Kaoru Okamoto, Director of Copyright Division, the Agency of Cultural Affairs, for his valuable advices.

(Original Japanese version: published in June 2002)