1. Copyright protection technology for digital content

The digital content distribution in current use is broadly divided between viewing digital broadcasting using a set-top box (STB) or TV set with a built-in digital tuner and viewing digital content on the Internet using a personal computer. From the perspective of the content user, there is no need to distinguish between digital broadcasting services and digital content distribution over the Internet. However, there are differences in the establishment of services based on TV broadcasting, which began under the guidance of a national policy, and the Internet, which arose through free thinking. Consequently, there are also technological differences.

2. Copyright protection technology

One of the main differences between digital and analog recording is that digital recording does not degrade the quality and further copies can easily be made from any copy. While these features are major advantages for the user, they make it possible for people to freely copy copyright-protected content for purposes other than personal use, which is not desirable from the viewpoint of a healthy content distribution market. Copyright protection technology is a technological solution for mediating between these two conflicting aspects.

Our aim is to utilize the advantages of both broadcasting and communication to develop an optimal hybrid system.

Examples of broadcasting and communication services are listed in Table 1, along with comparisons of encryption and copyright protection technology. The copyright protection technologies for digital broadcasting and Internet streaming that are currently the subject of standardization activities are compared in Fig. 1.

The copyright protection technology for current digital broadcasting can be broadly classified into conditional access systems (CASs), which restrict reception, and rights management and protection (RMP) technology, for which operation specifications are now being formulated. Reception restriction technology is the standard [1] used since the beginning of CS (communication satellite) digital broadcasting (subscription-based services) in 1996, but the scrambling of free-of-charge broadcasting services began in April of this year, with additional standards for BS (broadcast satellite) digital broadcasting [2]. The same kinds of systems are used for digital broadcasting, including terrestrial broadcasting, satellite broadcasting, and cable broadcasting (simultaneous retransmission of CATV (cable TV)), both in Japan.
and worldwide. On the other hand, digital rights management (DRM) has come to be widely used as copyright protection technology for streaming content on the Internet. Both of those approaches ensure secure viewing of copyrighted content within the range of authorized use, so they both have the same functions.

For subscription-based TV broadcasting, it is necessary to enable anyone installing a TV receiver to immediately receive the programs of any of the broadcast channels, as long as the viewing contract or other such preparation has been completed in the case of pay channels. For that purpose, TV receivers, including those for digital broadcasting, must be based on specifications for broadcasting systems that are standard, even among different broadcasters [3], [4].

For Internet distribution of content using personal computers, on the other hand, the user terminals (i.e., personal computers) vary in their performance, memory and storage capacities and operating system types and versions, and the user must install the application software required for each Internet service provider. Considering this situation, we believe that using standard specifications that extend communication func-

Table 1. Examples of broadcasting and communication services and comparison of encoding processing and copyright protection technology.

<table>
<thead>
<tr>
<th>Type</th>
<th>Storage*1</th>
<th>Transmission system</th>
<th>Service examples</th>
<th>Encoding processing technology</th>
<th>Copyright protection technology</th>
</tr>
</thead>
<tbody>
<tr>
<td>Broadcasting</td>
<td>No</td>
<td>Streaming</td>
<td>Terrestrial, BS, and CS are in service</td>
<td>Fixed reception technology</td>
<td>CAS: T</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>Downloaded file</td>
<td>Server-type broadcasting operation use being decided</td>
<td>(with scrambling) performed by CAS</td>
<td>DRM: Using DRM (capable of more detailed description than CCI)</td>
</tr>
<tr>
<td>Communication</td>
<td>No</td>
<td>Streaming</td>
<td>VOD</td>
<td>Implemented by same method as limited playback</td>
<td>DRM: Using DRM (capable of more detailed description than CCI)</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>Downloaded file</td>
<td>Download from server and store</td>
<td></td>
<td>DRM:</td>
</tr>
</tbody>
</table>

*1 Indicates whether or not the service providers assume local storage (excluding recording for private use)
BS: broadcast satellite
ACI: accounting control information
CCI: copy control information

Fig. 1. Comparison of rights protection system concepts for content distribution.
tions to current digital broadcasting is a realistic approach to cooperative broadcasting and communication services during the market establishment phase. From these viewpoints, server-type broadcasting, for which operation specifications are currently being formulated, is being studied on the basis of digital broadcasting standards [5].

3. Rights management and protection information

An overview of viewing licensing based on rights management and protection information (RMPI) is shown in Fig. 2. The order of operations is indicated by the numbers in the figure.

**Preparation for registration of content in the distribution center**

1. RMPI is obtained from the broadcasting company or other content owner.

2. If it is necessary to append RMPI that provides details within the range permitted by the RMPI of (1) according to the specific environment of the distribution network management function, then supplementary RMPI is defined and reserved. Of course, this supplementary RMPI may not contradict the permissions received in the RMPI of (1).

**Operational steps for when the user wants to playing the content**

3. The user makes a request to play the content. The playing request management function first confirms that the receiver is of the proper type for the content on the basis of the RMPI. Then, to protect the user, public key encryption is used for mutual authentication to ensure that the receiver is connected to a reliable distribution center.

4. On the basis of the user’s request, the pay request management function makes a request for license issuing processing.

5. The user’s contract is retrieved by the database management system to check for permission to view the content before proceeding to the actual licensing procedure.

6. The RMPI for the content that is relevant to the user’s request is obtained from the RMPI management function, and a license that reflects the conditions set in that information is generated.

7. The license is generated. At the same time, if the content has an associated charge, charging processing is executed. The receiver can then operate within the bounds of the issued license. For example, if the number of times the content may be played is specified, the TV set will present the content that many times, but no more unless the license is renewed. To increase the security level, the TV set can report the number of remaining plays to the content distribution center for checking just before each replay when a multi-play license has been issued, as a measure against unauthorized modification of the receiver.

Steps such as those described above ensure honest operation of the receiver according to the RMPI specified by the broadcaster. Typical RMPI items that are specifically needed for server-type broadcasting ser-

---

Fig. 2. Issuing of a license that permits viewing on the basis of rights management and protection information (RMPI).
vices or are assumed are shown in Table 2 and an example of the XML (extensible markup language) description for those items is shown in Fig. 3.

4. Future copyright protection systems

We have developed a rights protection system that meets the needs of a content distribution system based on cooperation between broadcasting and communication services. With recent technical advances—optical fiber, which can deliver the high-quality digital content of an HDTV (high-definition TV) program library via both broadcasting and broadband networks, large hard disk drives that can record and replay digital HDTV programs, and Blu-ray*1 discs for high-density digital recording—it has become technically feasible to draw up a true business model for broadcasting/telecommunication cooperative services.

In this article, we focused on how copyright protection information for digital content can be used in a business-to-consumer (B2C) environment, where digital content moves from the communication company to the user’s receiver. However, since the business-to-business (B2B) distribution of digital content among broadcasters and telecommunications companies must also be accompanied by copyright management information, the distribution of copyright permission management and digital content should be integrated. We believe that, in the future, mobile services involving AV (audio/visual) equipment, personal computers, and hand-held recording devices (cellular phones, PDAs, etc.) centered around a home server within the household will further enrich our lives. It goes without saying that copyright management of digital content use within the permitted range is necessary in this case too. We will continue research and development of the copyright protection technology and copyright management methods needed to support such a digital content distribution market.

---

*1 Blu-ray: A next-generation optical disc format jointly developed by thirteen leading consumer electronics and PC companies in Japan and other countries. It uses a blue-violet (wavelength: 405 nm) laser and can store 27 GB of data on one side of a 12-cm disc, which is sufficient for recording HDTV broadcasting directly in digital form. [http://www.blu-ray.com/info/](http://www.blu-ray.com/info/)

---

<table>
<thead>
<tr>
<th>Table 2: Examples of rights management and protection information.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content charge control</td>
</tr>
<tr>
<td>Control of copy generations</td>
</tr>
<tr>
<td>Control of number of copies</td>
</tr>
<tr>
<td>Control of the copying destination</td>
</tr>
<tr>
<td>Control of the number of playbacks</td>
</tr>
<tr>
<td>Time control of the playback function</td>
</tr>
<tr>
<td>Control of whether local storage is permitted.</td>
</tr>
<tr>
<td>Regional control</td>
</tr>
<tr>
<td>Gender-based control</td>
</tr>
<tr>
<td>Control over special playback features</td>
</tr>
<tr>
<td>Viewer age control function</td>
</tr>
<tr>
<td>Control of use by viewer attributes</td>
</tr>
<tr>
<td>Encryption processing specification control</td>
</tr>
<tr>
<td>Authentication processing specification control</td>
</tr>
<tr>
<td>Distribution media control</td>
</tr>
<tr>
<td>Control of number of distribution times</td>
</tr>
</tbody>
</table>
  <license licenseId="0">
    <title>TEST SAMPLE</title>
    <!--grant1 PLAY_SAMPLE-->
    <grant>
      <!--principal-->
      <right-->
      <nx:digitalContent>
        <nx:cri caBroadcasterGroupId="01" caContentId="0001">
          <nx:crid>crid://hoge</nx:crid>
          <nx:imi>imi:hogehoge</nx:imi>
        </nx:cri>
        <nx:SecurityInformation>
          <nx:EncryptionData>
            <nx:EncryptionAlgorithm>
              <nx:Camellia />
            </nx:EncryptionAlgorithm>
          </nx:EncryptionData>
        </nx:SecurityInformation>
      </nx:digitalContent>
      <!--condition-->
      <allConditions>
        <sx:fee>
          <sx:paymentPerUse>
            <sx:rate currency="JPY">100</sx:rate>
          </sx:paymentPerUse>
        </sx:fee>
        <sx:exerciseLimit>
          <sx:stateReferenceValuePattern>
            <sx:count>1</sx:count>
          </sx:stateReferenceValuePattern>
          <sx:stateReference>
            <sx:stateReferenceValuePattern>
              <sx:count>1</sx:count>
            </sx:stateReferenceValuePattern>
          </sx:stateReference>
        </sx:exerciseLimit>
        <validityInterval>
          <notBefore>2004-01-01T00:00:00+09:00</notBefore>
          <notAfter>2004-12-31T00:00:00+09:00</notAfter>
        </validityInterval>
        <tvax:distributionMedium>
          <tvax:FTTH />
        </tvax:distributionMedium>
      </allConditions>
    </grant>
    <!--grant2 COPY_SAMPLE-->
    <grant>
      <allConditions>
        <sx:fee>
          <sx:paymentPerUse>
            <sx:rate currency="JPY">100</sx:rate>
          </sx:paymentPerUse>
        </sx:fee>
        <sx:exerciseLimit>
          <sx:stateReferenceValuePattern>
            <sx:count>1</sx:count>
          </sx:stateReferenceValuePattern>
          <sx:stateReference>
            <sx:stateReferenceValuePattern>
              <sx:count>1</sx:count>
            </sx:stateReferenceValuePattern>
          </sx:stateReference>
        </sx:exerciseLimit>
        <validityInterval>
          <notBefore>2004-01-01T00:00:00+09:00</notBefore>
          <notAfter>2004-12-31T00:00:00+09:00</notAfter>
        </validityInterval>
        <tvax:distributionMedium>
          <tvax:FTTH />
        </tvax:distributionMedium>
      </allConditions>
    </grant>
  </license>
</licenseGroup>

Displays the crid of the target content.

Camellia is used for the encryption processing.

Charge is 100 yen.

Viewable one time only

Can be viewed between Jan. 1 and Dec. 31, 2004

Can be distributed by FTTH

When a different charge for the same content is specified, the details are described here.

Fig. 3. Example of XML description of RMPI.

References

Masahito Kawamori  
Senior Research Engineer, NTT Cyber Solutions Laboratories.  
He joined NTT Laboratories in 1989. He has worked in research areas such as artificial intelligence, language processing, and interactive agents using speech recognition. His current research area is metadata and media delivery systems for broadcasting and broadband communications.

Katsuhiko Kawazoe  
Senior Research Engineer, NTT Cyber Solutions Laboratories.  
He received the B.E. and M.E. degrees in engineering from Waseda University, Tokyo in 1985 and 1987, respectively. Since joining NTT in 1987, he has mainly been engaged in R&D of radio communication systems, satellite communication systems, and the personal handy-phone system (PHS). His specialty is forward error correction systems. He is currently a co-chairman of the Association of Radio Industries and Businesses Working Group for Broadcasting Systems based on a Home Server. He is a member of the Institute of Electronics, Information and Communication Engineers (IEICE) and received the Young Engineer Award from IEICE in 1995.

Sadakatsu Muto  
Promotion Project 1, NTT Cyber Solutions Laboratories.  
He joined NTT in 1989 and engaged in the developmental research on the database system supporting web services. Recently, he has been engaged in the development of copy protection systems for digital broadcasting and broadband communications.

Shinji Ishii  
Senior Research Engineer, Promotion Project 1, NTT Cyber Solutions Laboratories.  
He joined NTT in 1989. He is interested in developmental research on security systems for multimedia communications. Recently, he has been engaged in the development of copy protection systems for digital broadcasting and broadband communications.