Study Group on the Promotion of Digital Content Distribution, Telecommunications Policy Subcommittee, Telecommunications Council

Summary of Minutes (4th meeting)

1. Date: Tuesday, November 21, 2006, 2 to 3:30 p.m.

2. Location: Special Conference Room 1, Ministry of Internal Affairs and Communications

3. Attendees (honorifics omitted)

(1) Study Group members (including expert advisers)

Jun Murai (Study Group Chair), Nagaaki Ooyama (Vice-Chair), Tomoyuki Ikeda, Ryohei Ishii, Tsunetoshi Ishibashi, Yuu Inaba, Gota Iwanami, Yoshiyuki Uei, Naotaka Kacho, Makiko Kawamura, Junichi Kishigami, Nobuhiko Sato, Kazuo Shiina, Mizuo Sugawara, Yoshiyuki Seki, Nobuko Takahashi, Shinji Takada, Shuichi Tago, Mario Tokoro, Miwako Tsuchii, Fumio Nakajima, Miki Nagata, Akio Nosaka, Hidetoshi Haeno, Toshio Fukuda, Yoshitaka Hori (26 members)

(2) Observers

Masahiro Kamei (Japan Electronics and Information Technology Industries Association), Shin Kawase (Agency for Cultural Affairs), Yuuichi Tsubouchi (Japan Electronics and Information Technology Industries Association), Kichiji Nakamura (Japan Association of Music Enterprises), Shuichi Fujisawa (NHK), Keisuke Motohashi (NHK)

(3) Secretariat

Ogasawara (Head of the Content Distribution Promotion Department, Information Policy Division, Information and Communications Policy Bureau)

(4) MIC representatives

Suzuki (Director-General, Information and Communications Policy Bureau), Terasaki (Director-General for Policy Planning), Nakata (Deputy

Director-General, Minister's Secretariat), Fujishima (Director, Regional Broadcasting Division)

Murai (*Study Group Chair*) — Please allow me to open this, the fourth meeting of the Study Group on the Promotion of Digital Content Distribution under the auspices of the Telecommunications Policy Subcommittee of the Telecommunications Council.

Today's absentees are members Asano, Obuchi, Takenaka, Ichiya Nakamura, and Yoda. Also, as indicated in the handouts on your desks, we have six observers in attendance. Welcome to all.

The previous meeting dealt with the current state of content usage in foreign countries and related matters. At today's meeting, there will be reports and exchanges of opinions on matters relating to technologies brought up in our discussions so far that have been questioned or have been identified as requiring further confirmation.

First, I have requested explanations of the technical details of EPN [encryption plus non-assertion], a topic about which questions have been raised repeatedly since the outset of this Study Group's deliberations. Second, we will hear an explanation about the relationship between the so-called "B-CAS" [BS Conditional Access System] and "copy-once" technologies that I, and others, have referred to frequently.

With respect to our "homework" on conditions in other countries, which were discussed at the last meeting, basically we will prepare answers for the next meeting on November 27th, which is planned as a meeting on technology, and deal with those issues then.

First off, we will hear from JEITA [Japan Electronics and Information Technology Industries Association] on EPN and then from broadcasters on B-CAS.

Next, the Secretariat has compiled the questions that members submitted in advance and has distributed these to everyone as a handout. We will take up these questions and have a question-and-answer session after the explanation of EPN and B-CAS and before taking questions on those explanations. And as I said before, we will discuss the state of affairs overseas at the next meeting.

Before hearing from our speakers, I have a request concerning today's presentations.

The goals of today's discussions are to obtain the facts and to strive for a common understanding by everyone about technical mechanisms such as EPN and B-CAS. Despite limiting our topic today to technical matters, from past experience discussions are liable to touch on problems of private copying levies and systems as well as the details of past statements. Nevertheless, in order to make as much progress as possible on sharing facts about these technologies, I'd like to keep separate the many delicate discussions from today's session and deal with them at a later date. I realize it is difficult to keep these topics separate, but I ask for you to hold off on such discussions today.

Now, to begin, I'll ask Mr. Ogasawara from the Secretariat to go over today's reference materials.

Ogasawara (*Secretary and Head of the Content Distribution Promotion Office*) — Before I turn to the reference materials, today's agenda in front of you lists the names of the six observers we have here with us today, as Mr. Murai has mentioned.

If you turn to the agenda, you will find Reference 1, titled "The Framework of JEITA's Proposal on Content Protection for Terrestrial Digital Broadcasting," which consists of two pages, Reference 2, titled "RMP Enforcement and B-CAS," and Reference 3, a paper that lists some changes to our study schedule, which I will explain later on. Finally, there is a reference with no number on it. This is a summary put together by the Secretariat of the advance questions, as mentioned by Mr. Murai. I have handed these out just in case.

That's all from my side.

Murai (*Study Group Chair*) — Thank you. Now, Mr. Tago from JEITA will describe EPN for us.

Tago (*Study Group member*) — I am Shuichi Tago, chair of JEITA's Content Protection Study Group. I will give a brief explanation of the framework of JEITA's proposal, following along in Reference 1, which has been handed out to you.

There are two basic points to understand in the framework of JEITA's proposal on content protection for terrestrial digital broadcasting. These points actually originate from a proposal to another committee on terrestrial digital broadcasting, but here I will give them as JEITA's proposal.

The first is the necessity of understanding and preserving user convenience to enact a smooth and harmonious changeover from analog to digital in our terrestrial broadcasts, which are the key broadcasts in this country. The starting point of all our understanding is that the perspective of user convenience is indeed necessary to move smoothly to digital after terrestrial analog broadcasts are discontinued.

The second point — and there has been plenty of debate about this since the last meeting — is that for the manufacturers of receivers, the current situation is one where current content protection regulations — an example is TR-B14, an operational guideline for broadcasts established primarily by broadcasters — are presented to us and enforced by scrambling broadcasts.

Essentially, this is about enforcement — and this will probably come up with B-CAS as well. Since a B-CAS card is needed to unscramble the signals, broadcasts are enforced through the supply contract for B-CAS cards. Since this is basically about broadcast operating regulations, this is not a matter for JEITA to get involved with and the current understanding is that, as the Dharma is written here, our hands are tied.

Taking this as our premise and restating JEITA's proposal, the actual operational matters are the current copy-one-generation mechanism, commonly known as copy-once from the perspective of maintaining convenience for a smooth transition to terrestrial digital broadcasting. The broadcasting operation regulations, the actual operation of content protection regulated by TR-B14 I just mentioned, are technical operating standards and everything is written in them. The basic point of our proposal that we have been making since last year is: please, change these operations to use EPN output protection.

Next, if you turn to page 2, I'll quickly explain the comparison chart, as one of our goals, as Mr. Murai said at the outset, is to get the facts straight.

What this chart is comparing are the current analog and digital terrestrial broadcasts in Japan and, until they change, the same in the U.S. The last meeting focused on overseas trends. Please note that the situation in the U.S. is not settled, as

it is in the middle of a debate on a broadcasting bill. Therefore, I included the developments in the U.S. purely as a reference and as a comparison.

The first issue to look at is broadcast scrambling. Terrestrial analog broadcasts are not scrambled. Here, it says that scrambling is possible for terrestrial digital broadcasts. In Japan, this is possible by a ministerial ordinance. In the U.S., it is not.

Copy controls, naturally enough, do not exist on analog content. Currently, copy-one-generation control exists for terrestrial digital. At the same time, EPN is a type of copy-control information in terms of output protection, so I have included it here. The broadcast flag is currently under debate in the U.S.

Furthermore, the concept of enforcement doesn't apply to analog broadcasts because they do not include any copy-control information. As for terrestrial digital broadcasts, as I said just now, enforcement is primarily done through contracts, such as the supply contract for B-CAS cards. In the U.S., however, the obligations contained in FCC regulations are being debated. This enforcement is on the sending side.

Turning to devices next, I have compiled the relationships between recording functions and tuners that support recording functions.

As for recording media, the primary recording media is DVD. Analog tuners receive analog broadcasts, so there is essentially no limitation on recording functions. There are absolutely no limitations because analog does not contain copy-control information.

With terrestrial digital broadcasts, and including U.S. broadcasts, basically nothing can be used except authorized content-protection methods, to put it properly, given in operating regulations. A typical authorized content-protection method is CPRM [Content Protection for Recordable Media], which is for use with DVDs.

Number 2 is the issue of copying content to DVDs from hard disks. With analog, there are no restrictions whatsoever. With terrestrial digital, currently only moving is possible with the copy-one-generation scheme. On the other hand, EPN output protection does permit duplication by an authorized content-protection method but the copied content remains in a protected state; therefore, saying EPN has no restrictions whatsoever is not correct.

The next issue is dubbing. Here, dubbing means the further duplication of content that has been recorded on a DVD. Naturally, there are no restrictions at all

on dubbing terrestrial analog broadcast content. The copy-one-generation scheme for terrestrial digital broadcast content makes dubbing impossible. The no-more-copies flag prevents dubbing.

With EPN, as I outlined above, allows dubbing but in a protected state, so it does have some limitations.

Below this is the issue of playing content recorded on a DVD. In other words, this is about whether the content can be seen on a player. All terrestrial analog broadcast content can be viewed from DVDs. Since terrestrial digital broadcast content generally incorporates protection mechanisms, it can be viewed on players that support the protection mechanism of the DVD media. Putting it the other way around, a DVD cannot be played on a player that does not support the DVD's protection mechanism. This is point Number 4.

The final issue is whether recorded programs can be transmitted in a viewable state over the Internet. This is physically possible with terrestrial analog broadcast content, but naturally unrestricted transmission over the Internet is against the law. In contrast with this, it is not possible to transmit terrestrial digital broadcast content over the Internet in a viewable state. This is described in Note 2, but I will go over this in more detail later. Debate on this issue is still ongoing in the U.S., but it seems like a certain few number of transmissions will be recognized.

This concludes my explanation using the comparison chart of analog and terrestrial digital issues, and for reference the U.S. conditions, that many of you have had questions about.

To continue to respond to other questions you had, we will have a more detailed explanation about enforcement issues and, as I mentioned earlier, about the inability to transmit content in a viewable state over the Internet.

Tsubouchi (*observer from JEITA*) — I am Yuuichi Tsubouchi, a member of JEITA's Content Protection Study Group. I'd like to give an extra explanation using the projector of the details on the back of page 2 that Mr. Tago has just described to you.

With this reference, I hope to use illustrations to explain as clearly as possible the TR-B14 operational guidelines for broadcasting from the perspective of how we manufacturers understand them and how they are handled on the device side.

First, here is page 1. This describes the relationship of scrambling and copy control in terrestrial digital broadcasts.

The top half in the center of the screen is the enforcement framework in Japan and, for reference purposes, the bottom half shows the enforcement framework in the U.S. broadcast flag regulations. I'll introduce this topic by contrasting the two frameworks.

First, please look at the illustration showing the sequence of events in the center with the Japanese flag. The TV tower on the left transmits the broadcast signal, which is received by the receiver. The program is then stored on the hard drive built in the receiver or else the signal is output from the receiver.

The broadcast station transmits copy-control information, such as copy-one-generation, that is multiplexed with its broadcasts. This is done on a program-by-program basis. In this case, copyright protection is realized with the receiver correctly handling this copy-control information and recording or playing the content at the receiver in accordance with the copy-control information and, thus, with the intentions of the program sender. The broadcast signals are scrambled in Japan, however, to place the obligation on receivers to correctly support copy-control information and to enforce this obligation.

The specifics of this are explained in the square box. A B-CAS card is necessary to unscramble the broadcast signals. Thus, the obligation of receivers to adhere to the content-protection rules is enforced through contract when the B-CAS cards are supplied. In other words, B-CAS cards can only be installed in legal receivers that comply with content-protection guidelines and properly support copy-control information, and only these receivers can unscramble the broadcast signals. This is the enforcement framework in Japan.

In this picture, the digital outputs and the built-in removable media of the receiver are depicted in red. When someone attempts to output digitally or to record or store on the removable media a broadcast program that the copy-control information indicates as protected, there are regulations that say protect this content using this protection mechanism, or conversely, you can't store or output this content without using this protection mechanism. These regulations are written in the TR-B14 content-protection guidelines. The framework also includes the D-PA

[The Association for Promotion of Digital Broadcasting], which authorizes protection mechanisms.

Below this, for your reference, is an illustration of the enforcement framework contained in the U.S. broadcast flag rule. As our guests from the Mitsubishi Research Institute described at the last meeting, under the broadcast flag rule, broadcast stations assert the broadcast flag in programs that are to be prohibited from being redistributed in mass indiscriminately over the Internet and other networks. The broadcast signals, however, are not scrambled and are transmitted in so-called plain-text format.

Asserting the broadcast flag, however, is meaningless if no receivers see the flag or else they see it but ignore it. Therefore, the enforcement framework uses laws and regulations — specifically obligations made under FCC rules — to ensure receivers detect the broadcast flag and protect the broadcast program accordingly. The broadcast flag framework also relies on the FCC to judge and authorize the protection technologies used in receivers to govern digital output and storage.

What I've described is the manufacturers' understanding of the relationship between scrambling and copy control in terrestrial digital broadcasts.

On the next page, we'll look at the mechanism that protects broadcast programs after they have been output digitally or stored on a removable media from the receiver using an authorized protection method.

After a broadcast program has been output digitally or stored on a removable media from the receiver using an authorized protection method, the broadcast program is protected by a chain of contracts with the original protection method, as the title here suggests.

More specifically, in the Japanese framework, the broadcast program is handed off after being securely stored or output from one protection method authorized by the D-PA to another protection method that the original protection method recognizes. When such a transfer happens, the upstream side, the side handing over the program, sets rules, the broadcast program's copy-control information, that are inherited by the downstream side, the protection method of the device accepting the program.

Now, look at the middle illustration. This shows an example, starting from the left, of a receiver receiving a protected program and then outputting the program

over a digital-signal cable to a DVD recorder, which records the program on DVD media.

Now look at the very top illustration. The receiver on the left is built in compliance with TR-B14. So when a program is output digitally from the receiver, a protection method must be used that is listed as an authorized protection method in TR-B14. Here, as an example, the broadcast program is output while protected with DTCP [Digital Transmission Content Protection], since DTCP is a recognized protection method.

Next, the program is transmitted along the signal cable while protected by DTCP and received by the DVD recorder. After receiving the program, what protection method must be used when recording the program to DVD is stipulated in the DTCP licensing contract. In other words, the DVD recorder can only record to DVD using protection methods recognized by DTCP. In this example here, DTCP recognizes CPRM.

In this way, broadcast programs are securely transferred from one authorized protection technology to another protection technology recognized by the first protection technology. This is shown by the illustration in the center with green, blue, and red crosshatching. The content is re-encrypted each time it is transferred and the copy-control information is passed on from the passing side to the receiving side like a bucket brigade.

In the example here, the copy-control information, EPN, attached to the broadcast signal is first passed on to the EPN defined by DTCP and then passed to the EPN defined by CPRM when the program is recorded with CPRM.

Consequently, as is written in the balloon on the left, when some new copy-control information is defined upstream, it is necessary to achieve consistency throughout the chain, such as how the copy-control information will be passed to the next level, and how it will be passed from that level to lower levels. Thus, such modifications require revisions of the protection method standards at downstream devices.

Next, for your reference, is a diagram of the U.S. broadcast flag rule at the bottom of the page. As I explained before, broadcast signals are not scrambled and are transmitted in plain-text form, but after detecting the broadcast flag receivers must use an FCC-authorized protection method when outputting signals digitally.

In this example, the broadcast program is output while being protected by DTCP, since DTCP is recognized as it is in Japan. As for the copy-control information, EPN is added just like in the upper illustration. Following this, the DTCP licensing contract stipulates whether it is okay to pass the broadcast program to another protection method. If okay, the copy-control information is passed on through the EPN defined by DTCP. Thus the protection of broadcast programs once they are output digitally from the receiver is the same as the EPN operation in Japan shown in the upper illustration.

This describes the manufacturers' understanding of the chain of contracts between protection methods.

On the final page, I'll describe the methods by which broadcast programs are protected after being recorded on media and how broadcast programs are prevented from being transmitted in a viewable state over the Internet.

The most important point to understand about the protection mechanism for broadcast programs recorded on removable media is that the broadcast programs are encrypted before being recorded and that the encrypted information is bound on a one-to-one basis with the media it is written to. In other words, the content is encrypted and recorded separately for each media disk. Therefore, the original media disk to which the encrypted program is bound to is always necessary in order to decrypt the program. If the recorded program is separated from its original media disk, it cannot be played or viewed.

Look now at the dotted box on the left where "Record" is written. In this example, a recorder supporting protection method A is used to record a broadcast program on media that also supports protection method A. To encrypt and record the broadcast program on the media, a device key and a media ID are necessary. The device key is unique to the recorder and is provided to the manufacturer of the recorder from the licensor of protection method A. The media ID, shown in blue here, is a unique identifier recorded on the actual media disk.

The media ID is written on the disk or removable media in the manufacturing process. The "x" written here represents the unique ID number of each media unit. The media ID cannot be duplicated or altered in any way.

The recorder uses the device key, the media ID, and other data — shown in yellow on the bottom left, to generate the encryption key — at the bottom left in

green — for recording the broadcast program to the media. This key, in effect, locks the green padlock on the encrypted recorded file. The exact same key as the green key at the bottom left must be generated to unlock the padlock, decrypt the encrypted program, and watch the program.

Next, how such a recorded broadcast program is played back is explained in the center dotted box labeled “Play.”

Can media IDx be inserted and played in a player that supports protection method A? Well, because the player supporting protection method A has the green device key, it can generate the same key used when the program was recorded — the green key in the center — using the device key and media IDx on the media disk. Consequently, using this key, a player supporting protection method A can unlock a protected and encrypted program on a media unit with IDx and then play and view the program.

The pink area in the upper right shows what will happen should the encrypted program file recorded on media IDx be transmitted over the Internet. Here the media is put in a computer drive and the encrypted program file is ripped from the media and sent over the Internet. On the receiving side, the encrypted program file is taken and recorded on another media disk that supports protection method A.

The media ID of this second disk that supports protection method A is shown in red as “y.” But can the encrypted file recorded on media IDy be played on the same player that supports protection method A that could play the file from media IDx? Well, this time the player has the correct device ID but since the media ID is now y, the player generates a key that is different from the key used when the program was originally recorded. Therefore, the encrypted file cannot be unlocked and the content cannot be viewed. This means if someone tries to pass the broadcast program encrypted and recorded on media IDx to someone else over the Internet in a format that can be played back, the person would also have to send the actual physical media as well.

The current mechanisms that protect broadcast programs when recorded on media use this type of encrypted recording that binds the broadcast program to a specific media disk and in this way creates an environment where broadcast programs cannot be played or viewed when separated from their original media disk and prevents the content from being transmitted over the Internet in a viewable state.

That concludes my discussion of these topics from the understanding of manufacturers.

Murai (*Study Group Chair*) — Thank you very much. Next, Mr. Seki will continue on about B-CAS.

Seki (*Study Group member*) — I sense that in your very thorough presentation you have already touched on most of the points I was planning on talking about. Still, D-PA came up in the past discussion, so I'd like to speak about it and about the BPA [The Association for Promotion of Satellite Broadcasting], which both essentially regulate the same content protection guidelines, including BS [broadcast satellite] broadcasting. I, Yoshiyuki Seki, serve as the chair of both the D-PA's and BPA's technical committees.

I expect that today we will be going into quite a bit of depth on these points, so I'll be asking for assistance from Mr. Fujisawa from the NHK, who is here with us today. Mr. Fujisawa was responsible for examining and creating the guidelines of both organizations particularly on content protection and as such is much more knowledgeable than me.

Before then, allow me to explain about RPM [rights protection management] enforcement and the B-CAS method that previously people have had questions about.

I'll be explaining while following the nine-page reference I've prepared.

I don't think there are any page numbers, but if you turn to the first page after the cover, you will see that "Transmission Operational Rules (DTCP Encoding Rules)" is written at the top. I'd like to speak a little here about how the rules came into existence, as I'll be mentioned things related to this later on.

First, this DTCP protection method came to be employed basically around the start of 2000, just after BS receivers had been standardized. I remember that the DTCP rules at this stage did not include anything about free broadcasts with content protection, as given in the second point from the top. In other words, copy control was applied to pay-per-view and monthly pay-TV broadcasts but not generally to free broadcasts. Although this was explained earlier, the DTCP rules included DTCP encryption, despite, as I heard, encroaching on some patents, and because

this came to be used, no controls at all were placed on free broadcasts. This exception to the above is explained in the bottom line.

At this stage, some expressed a desire to apply copy controls to BS free broadcasts as well, and broadcasters discussed the DTCP structure with device manufacturers. As a result, I think it was in 2001, the line about free broadcasts with content protection was added to the rules.

Below this is one application method known as free conditional access delivery. At the time broadcasters were hoping to add this method to their broadcasts and thereby affect copy control.

The main point of discussions on free broadcasts with content protection was the content protection itself, and the discussion basically turned to using scrambling to realize content protection.

Paid broadcasts had already started in October 2000 and these were scrambled of course. At the time, copy-one-generation or pay-per-view did not exist, so I don't believe copy prohibition existed then. Essentially, the rules governed operation when content was used.

One more point I want to talk about is the figure on the rightmost side labeled "output protection." Where *2 is written, this is where operation is possible only when unconditional copying is permitted. Unconditional copying, that is when CCI [copy-control information] is 00, corresponds to the circle on the far right where output protection is applied when using the column on the far left in the so-called third-generation restriction. When we talk about EPN, we are talking about this operation.

Therefore, although copy-one-generation is in fact in operation, today EPN is still in the operational rules.

Going back a bit, free broadcasts at that time were not scrambled. This meant that everything could be unconditionally copied. Therefore, people began wanting to use some sort of COG [copy-one-generation] technology and, after much debate, the free broadcasts became scrambled, in a word, for enforcement. This sequence of events is spelled out on page 3.

Next, regarding rights protection information, or CCI, devices that supported the DTCP mechanism at that time could protect rights but devices that didn't

support DTCP didn't protect rights. Thus, debate began about how to guarantee that this DTCP method would be employed.

This led to the issue of enforcement of rights protection information. People realized that even if copy-control information, that is rights protection information, were transmitted, the details of this rights protection information would not necessarily be protected on the receiving end. Therefore, for reliable and certain rights protection of broadcast content, rights protection information would have to be transferred reliably not just to receivers but to other downstream devices that connect to receivers, such as VCRs and hard-disk recorders, in succession, as was mentioned previously. But if there were no enforcement to make receivers observe rights protection information, not only would rights protection methods be ineffective; it could lead to unfair competition that would unduly punish honest manufacturers. Although talk of legal enforcement came up in discussions with mass manufacturers, in the end the parties went in the direction of technical enforcement. Signals would be scrambled and receivers that properly observed rights protection information would be given keys to descramble broadcasts.

Next, I'll speak about the basic policy that was adopted when examining protection schemes. Examinations began in 2001 when a study group was set up under the Telecommunications Council. The first precondition to the examinations was that the protection scheme had to be compatible with existing digital broadcast receivers and that it had to be a cross-media rights protection scheme for all media meeting the requirements.

The second precondition was about server types and so forth, which I'll leave out because it isn't relevant to our topic.

At the time BS receivers were already on the market; hence the precondition that the rights protection method had to be compatible with these receivers. This led to the adoption of the present-day B-CAS scrambling method.

In line with the basic policy of the examinations, this method realizes rights protection by adding necessary functions to the existing broadcasting method. This was done for compatibility with the existing broadcasting method. Assuming that the existing digital broadcast receivers were BS broadcast receivers, the biggest issue was finding a rights protection method that these receivers could support using their existing built-in functions. In other words, since BS receivers were already on

the market at the time, if an incompatible content-protection method were adopted, these receivers would no longer be able to receive the broadcasts. This was untenable, so the functions of the existing receivers had to be carried on and so the B-CAS method was carried on.

The next page deals with content protection methods. As was said earlier, broadcasters, in principle, can select from three types of copy control — copy-free, copy-one-generation, and copy-never — with the copy-control information (CCI). This is specified with the two-bit CCI code. Furthermore, the entire program is scrambled and broadcast. Now, as shown on the right, receiver manufacturers request the B-CAS organization to supply them with cards for their receivers that have secure copy-control functions. B-CAS supplies cards to the manufacturers, who then package them with their receivers. As written on the left, when the B-CAS card is inserted in the receivers, you can view broadcasts as normal, but without the card, all you see is the scrambled signal. Broadcast content is controlled based on the CCI signal once it has been received. The bottom section shows the process after content is received.

Next is a summary of how the B-CAS, the company, was established. The company was originally set up to unify management of the CAS method for BS digital broadcasts and particularly paid broadcasts. It was established in February 2000 and, as the shareholder ratio written here indicates, its main investors are BS broadcasters and vendor operating companies.

The next page gives the aim of setting up the B-CAS company. To repeat myself, the company was established on the basis of unifying the CAS management of WOWOW and other paid broadcasters that existed at the start of the BS age.

Following this aim, B-CAS was set up as a company that unified the operation and management of the common infrastructure of digital broadcasts, today BS and 110 CS, and limited reception systems like cable TV. Now, as written in point (2), copyright protection and bidirectional services have been added to this. While bidirectional services are almost never used, today B-CAS is generally used to unify the management of paid broadcasts, auto-display messages, and copyright protection.

The final page shows the basic sequence of B-CAS operations. This repeats some of what I’ve talked about. Starting on the top right, B-CAS requests a card

vendor to create cards and add an encryption key. After getting the finished cards, the B-CAS company supplies the cards to manufacturers of receivers that meet the conditions for supplying the cards: specifically, as was outlined previously, properly implementing content protection. These cards are bundled with the receivers.

Broadcasters use RPM broadcasting, which refers to scrambling programs and encrypting with CAS. Basically, if the receiving party has a receiver made by a manufacturer that properly protects content, the receiver will have a card with it. Inserting the card unscrambles the broadcast signal and allows the broadcast to be viewed.

Finally, please turn back three pages. Here is an illustration of the content protection method. As I said a little earlier, the purpose of the B-CAS card and scrambling is only to enforce that the receiver is implemented so that it enacts content protection properly as specified by the CCI. Thus, the signal is scrambled and the B-CAS card unscrambles the signal.

There has been a lot of talk of “moving” content, COG, and EPN. All of these are ways of handling content after it has been received. From a technical standpoint, this is essentially a separate topic. What to remember is that control based on CCI is a sort of request included in broadcasts sent from here to the receiving side, and to ensure receivers properly follow this request, the signal is scrambled and then unscrambled with the B-CAS card. I’d like you to understand that enforcement and the actual operations of content protection are separate topics. Thank you.

Murai (*Study Group Chair*) — Thank you very much.

Before we move on with questions about these presentations, I’d like to start with the questions that were submitted in advance. To move through our discussions efficiently, I will nominate the respondents and should a question be difficult to answer here today, I will discuss how to handle the question later with the Secretariat.

In your reference you will see questions numbered 1 to 8. The last two relate to developments overseas so, as I said at the outset, we will deal with these at the next meeting.

Some of these may have been touched on in our presentations just now, but I will ask Mr. Tago to respond to questions 1 through 4.

Tago (*Study Group member*) — Okay, I'll start from the top.

First, question 1: Is content recorded in high definition or standard definition on DVDs? Well, DVDs were originally in standard definition, so here they are recorded in standard definition.

The details below the parentheses are not really for a manufacturer to address. So, if you can, Mr. Seki, would you answer this?

Seki (*Study Group member*) — I see. As broadcasters see it, there is absolutely no distinction operationally of whether recording controls apply when moving a program recorded in high definition to a DVD in standard definition. This has never come up in discussions so it's a little hard to say, but thinking the other way around, there is some question of whether such a distinction can be made on the hardware end. Essentially there has been no discussion about moving from high definition to standard definition or which is which. So currently no distinction is made.

Tago (*Study Group member*) — Next, question 2.

Are there products already on the market that move content in high definition? Well, there are three types on the market. The first point is that when moving from an internal hard disk to an external, or standalone, hard disk, it is possible to record in high definition. So, yes, there are devices on the market that can record in high definition while moving content.

More recently has been what's known as next-generation DVDs. There are two formats: HD DVD and Blu-ray. These are both optical disk media. These too are already on the market.

In terms of prices, hard disks are undoubtedly the same as hard-disk recorders. The next-generation DVDs that record in high definition, looking at real market prices, appear to be higher. That is the second point.

Proceeding on to the third question, there is a movement to get rid of all devices, in short DVD recorders, that record moved content in standard definition by 2011. Whether this will happen or not, it's hard to say. In the end, this is basically left up to the business judgment of manufacturers, so I can't really answer this question. At the very least, however, there are a huge number of DVD recorders

already out there, and we can assume that a large number will still be around in 2011.

Incidentally, I checked the statistics on the number of DVD recorders shipped. JEITA's stats lump analog and digital in together, but the total number of DVD recorder/players shipped so far is around 14 million, and there are more not included in these stats. Of these, there are about 2 million units with built-in terrestrial digital tuners. These are real figures, the number that have actually been shipped according to JEITA stats and this will increase from here on. Therefore, we can assume a large number will still be around in 2011.

The fourth question is about recording on video decks — those with the three-color cables, red and white for audio and yellow for video. While naturally they record in analog, they are capable of recording digital broadcast content.

That's all I have.

Murai (*Study Group Chair*) — Thank you very much.

Question (5) may overlap on what we have just heard, but Mr. Tago, if you please?

Tago (*Study Group member*) — Today, Mr. Kamei, chair of JEITA's copyright committee is here with us, so I'd like to turn this question over to him.

Kamei (*observer from JEITA*) — I am Masahiro Kamei, chair of JEITA's copyright committee, and I'm here today as an observer.

One point about question (5). We've heard about the technical side of copy-free, but I'm inclined to think that this borders on piracy. Let's consider what pirated versions mean. One form is so-called systematic piracy done by professionals. But what we are looking at today, COG or EPN, doesn't really involve the activities of these professional pirates. Instead, what I'm conscious of is whether there will be calls to consider the making of duplicates or recordings with COG and EPN in the home as piracy.

It is definitely illegal to sell or auction any recording of broadcast content you have made. And the distribution of recorded programs over the Internet isn't

relevant to the conversation because, as we have heard, it is technically not possible. So the problem, as I see it, is this sort of transferring between media.

If we take the current behavior of consumers — and I think this is the vast majority of consumers — who are not involved in piracy or auctioning or other activities when, for example, media is generated with COG, and then use this behavior as the basis for hypothetically allowing a certain number of duplicates with EPN, I believe we have to account for the possibility of an increasing number of illegal copies appearing.

I think we all agree that most people who have never been involved with piracy are not likely to start pirating the copies they have in front of them. For JEITA then, it's a huge problem to place restrictions on and inconvenience the vast majority of sensible users all because of the acts of a few unscrupulous malcontents.

That is my position.

Murai (*Study Group Chair*) — Thank you very much.

Question (6) concerns B-CAS. Mr. Seki, over to you.

Seki (*Study Group member*) — There are four points to my answer. Point 1 has essentially already been covered in the previous explanation. Point 2 is the biggest point about the cost issues with the B-CAS cards. Will viewers have to bear the costs of operating B-CAS? The short answer is no: the viewers will not directly bear the B-CAS costs. Broadcasters and manufacturers will separately undertake the costs. Now, you can argue that, much like ad-sponsored broadcasting, in the end the costs will be transferred to the viewers, but the viewers do not directly pay for the costs of the cards.

The third point is about adopting EPN. Under the current DTCP rules, B-CAS would be necessary as explained earlier.

The fourth point is that B-CAS was originally a mechanism for paid broadcasts. The answer then to why is it being used in free terrestrial broadcasts is that free terrestrial broadcasts are scrambled for enforcement reasons through the sequence described before, and B-CAS was employed because it had been in use from the start.

Tago (*Study Group member*) — Mr. Seki, if I may. If manufacturers bear the costs of B-CAS cards, as you said, then manufacturers lease these cards?

Seki (*Study Group member*) — That's right. They do not pay for the cards.

Tago (*Study Group member*) — I'm just making sure they are not paid for. The hardware associated with B-CAS is naturally paid for by the manufacturers.

Murai (*Study Group Chair*) — About point 3 that you just made, if EPN is adopted, B-CAS will be necessary, right? In other words, we had an explanation that B-CAS is an enforcement mechanism. Is that explanation consistent? In Mr. Tago's description, B-CAS is the enforcement part and EPN is the technology for output protection. Is what Mr. Seki said about Question (6) part 3 correct?

Tago (*Study Group member*) — As far as manufacturers understand it, enforcement is essentially ensured through the B-CAS contract because it is included in the operational guidelines.

Murai (*Study Group Chair*) — Technically, are they independent?

Seki (*Study Group member*) — They are completely independent, but the idea of scrambling for enforcement when EPN is in operation is the same as for COG. Thus, if we adopt EPN, that does not mean that scrambling is no longer necessary.

Murai (*Study Group Chair*) — Is that an operational problem?

Seki (*Study Group member*) — Well, you can say it's operational, but this is because the DTCP rules say that enforcement will be done with scrambling.

Murai (*Study Group Chair*) — Is there anyone who needs more explanation on this point?

Tsubouchi (*observer from JEITA*) — Can I make one point? What's being said now is that B-CAS is necessary if we go to EPN. Indeed, on page 2 of the reference, as the DTCP encoding rules, the transmission operational rules, are written in Japan's TR-B14, if EPN were introduced, then B-CAS would be necessary with free broadcast programs that have content protection. In other words, it's necessary to have enforcement through scrambling. But if we think of DTCP, that is the encoding rules in the licensing agreements, as being independent, EPN could also operate by placing a framework where response to a flag, like the broadcast flag, was made obligatory by law between the free broadcast programs that have content protection and the DTCP. In other words, we could have encoding rules that say it's okay to trigger DTCP with EPN, and a broadcast operation equivalent to one broadcast flag could be included between these two schemes.

Seki (*Study Group member*) — I explained that at the last meeting. I also explained that later the rules became what they are. When the rules were decided there were no broadcast flags or other frameworks. Plus, there was a huge debate at the time about the FCC rules and there was talk of regulations with exactly the configuration you are describing. And there were also descriptions of what might happen if we went the legal enforcement route.

Tsubouchi (*observer from JEITA*) — That's correct.

Seki (*Study Group member*) — There was a lot of discussion about whether we could use legal enforcement. Even the government was involved in the debate. In the end, we decided it was too difficult and took the technical enforcement route that we use today.

Murai (*Study Group Chair*) — Is everyone fine with that? Okay, let's go ahead with your questions and discussions about today's presentations.

Shiina (*Study Group member*) — At the last meeting at the start of your presentation I asked this, but I don't think there was any explanation about the core of this

discussion, moving content. I'd like to hear more details about move failures, how the rules of move are defined, and how the move function is implemented.

Tago (*Study Group member*) — This is for Mr. Fujisawa because it deals with the operational rules.

Seki (*Study Group member*) — Once BS broadcasts got underway, there was a great deal of discussion about content protection, including COG. This actually took place in May 2001, with 8 BS companies and all the 5C manufacturers except Intel. The meeting was called the 8B4E. At that time, the four manufacturers submitted a plan and that called for a move function.

In the context of the DTCP rules, move was restricted to only no-more-copies content. Furthermore, each move would be done only for one recording media unit, and the previous file before the move could not exist at the same time as the usable copy after the move. This is how the move function was proposed in the context of the DTCP rules.

At the time, the manufacturers proposed a whole set of rules, not just the move function. In the end all of this was called 8B4E and about a month after the broadcasters and manufacturers reached an agreement, they began working on the premises of the guidelines. That's the history of it.

Shiina (*Study Group member*) — I already know the story of the mechanism. Move only works with content that is recorded as no-more-copies. And after moving the content to the other media, the two copies cannot exist simultaneously. But more specifically, for example, when you move a program from a hard disk to a DVD, why do move failures occur? That's what I don't understand.

When you write to an optical media, normally you confirm the written data physically with a verify or compare operation and then erase the original file. That's the normal case. But if this verify operation isn't implemented, why do you continue to advocate the move function?

Murai (*Study Group Chair*) — So the question is not asking about the operational rules but about the implementation.

Tago (*Study Group member*) — I can't answer because this is written in the operational rules.

Murai (*Study Group Chair*) — But this question is not about the operational rules, it's about the implementation of the move function.

Shiina (*Study Group member*) — Yes, I am talking about implementation. In short, the user buys a device that can move content and then tries moving content. When the move operation fails, is this a problem with the DTCP or other rules that you have taken great pains to explain or is this a problem with the implementation technology? I want to where the problem lies.

Murai (*Study Group Chair*) — He wants an answer along the lines of is it technically impossible to commit to the guidelines, whatever the rules were when the operational guidelines were decided. Can someone explain this?

Shiina (*Study Group member*) — Since manufacturers build the devices, I'd like a manufacturer to explain.

Tago (*Study Group member*) — I've been reading the TR framework. Please understand that manufacturers build their devices in line with this framework. The reason is for enforcement.

The move function is given in Section 8. Content can be moved to one recording media either built-in or connected digitally. So when moving content over a high-speed digital interface, such as iLink, to another recording media, it must be done in line with the DTCP rules. What this is saying is "Follow the DTCP rules over iLink." The section also says that move operations cannot be done to analog devices or media.

The next regulation is that during the move operation, no playable content over one-minute long can exist simultaneously at both the move source and the move destination. So move operations are implemented in line with this regulation.

Next, after the move is over, usable content cannot exist simultaneously at both the move source and the move destination. In other words, after the move is completed, the content at the move source must be made unplayable. The section has lots of other details about disabling the playback of content, which is also in the move function. Basically, manufacturers implement the move function in adherence to the wording in the broadcast operational guidelines without making a fuss about it. That is as far as I can answer.

Shiina (*Study Group member*) — I have one more thing to add. If that's the case, we don't know anything. In short, I bought one, a hard-disk recorder. Normally when you transfer data to an optical disk or other peripheral, there is some technology like verify or compare in place. Despite this being the normal situation, from what you are saying, am I right to understand that when I move content, because of all these regulations in the TR, this technology is not employed?

Tago (*Study Group member*) — Mr. Seki. Can I ask you to answer this?

Seki (*Study Group member*) — From the point of a broadcaster, broadcast technicians have no idea whether this sort of thing can be done, so we went to the manufacturers and asked "Can this be done?" And after consulting with the manufacturers, what they are building conforms to the TR. In the end, the wording I gave you came about. So about what Mr. Shiina is asking now, if the manufacturers are building their devices in accordance with this wording, then basically I think this is not true.

Motohashi (*observer from NHK*) — Listening to what has just been said, I think Mr. Tago's assertions are nothing more than exceedingly formal logical constructions. As Mr. Seki has just said, since the operational guidelines of broadcasts are inextricably linked to the receiver specifications, naturally these guidelines are not decided completely by the broadcasters. There are lots of conversations with the receiver manufacturers and we tell them we want to do such and such and ask what technical solutions are there to do this and the manufacturers give us suggestions and advice. This is how the rules came to be. So seriously debating about what the

explanation is all about — that the broadcasters made the rules and thus we don't know anything — is a bit of a taunt really, though everyone's positions are different.

This is slightly off topic from what Mr. Shiina is interested in, but scrambling and B-CAS enforcement came about because of a desire on the part of the manufacturers to exclude devices that did not support the rules. I don't think the discussion to this point touched on this. So including this, what I'd like to say is that we need an accurate disclosure of information for debate in this venue, since today, for example, we are to obtain a common technical understanding. To be sure, I'm not advocating an exceptionally detailed conversation.

Murai (*Study Group Chair*) — Thank you. Next, Mr. Takahashi.

Takahashi (*Study Group member*) — I've been listening and I understand that the rules were determined through various conversations between the manufacturers and the broadcasters. But at the outset, JEITA showed the picture of the Dharma, which gave me a fright. It's not that your hands were tied, as you suggested, but that you hid your hands.

I was involved with the third interim report because I am a member of the Telecommunications Council. This report clearly outlined the background to the copyright protection implemented by the technology called DTCP. DTCP is a technology that protects content during transfers between digital devices over digital interfaces. When using this technology, it's required to adhere to the operational rules of the technology, which are called the encoding rules. This technology was jointly developed and established by a group of manufacturers called 5C. And 5C created the operational rules after consultations with the U.S. movie industry. All of this was clearly written in the report. So, when you say that your hands were tied, we are left very perplexed.

I think broadcasters have some responsibility for this too, but as a consumer, I am dumbfounded by such extremely irresponsible discussions. It's not about who did what; it's about greatly inconveniencing the consumers. For example, the report clearly spelled out issues with the move function. Based on the indications that when a move failure occurs neither the original broadcast program nor the broadcast program partly recorded on DVD can be used, the report called for an examination

of concrete measures at the receiver to address this issue and to report on the state of these examinations by December this year or sooner if possible. So though we've had a very specific explanation of the bucket-brigade system, consumers have pointed out issues that the bucket-brigade system isn't up to scratch. So if we don't have a productive discussion leading to an answer to this, we will just be repeating the same mistake as last year. I think it's very wasteful that more than two years will have gone by.

Continuing on about the encoding rules, people were asking at the Telecommunications Council, and I'm sure this was said by more than one member at the start of these discussions, are there no other rules other than the four — EPN, copy-free, copy-never, copy-one-generation — for there must be other rules? If this isn't cleared up quickly, the ones who will be hard pressed will be the broadcasters and the manufacturers. Because consumers won't use what they find difficult to use.

That's all.

Shiina (*Study Group member*) — I was musing about your answer just now, and what I hear you saying, in short, is that neither side is responsible. One thing that is clear is that it has been done in the context of DTCP following the operational rules decided by the ARIB. When a device that is sold to a user on the condition that it will behave in such and such a way in the context of these rules and then doesn't behave in such and such a way, who is responsible? That is what I want to clarify here, because it is not the responsibility of the copy-once rule.

Plus, in the explanation of EPN, which for some reason was done on the display and not with handouts, we heard content is locked with a key generated by combining the media's key and the content's key. And when burning a DVD or whatever from the hard disk, the same key is generated. It wasn't written that the same key is created each time another copy is made, but surely it is the same key. On the Internet, the media ID changes so the content cannot be unlocked. I completely understand this, but the logical conclusion of this explanation is that there are no restrictions on copying to DVD from hard disks. And what are we to think about generations can be made without restrictions from the DVD copied from the hard disk? Rights holders can only look at it as being the same as copy-free.

On the other hand, rights holders cannot help but have some suspicions about the specifications of the devices capable of moving content that are now on the market based on the copy-once rule — and note I'm not saying suspicions with the copy-once rule itself.

Murai (*Study Group Chair*) — Are we comfortable with the understanding in the first part of this statement?

Seki (*Study Group member*) — I think what Mr. Shiina and I are questioning is that the last figure is not very clearly shown. What exactly does it mean to be copyable in a protected state, as Mr. Tago said? Almost everything that comes out is in this protected state.

I don't sense there has been answer to the statement that in the end, copies can be made regardless of generation restrictions or restrictions on the number of copies. We understand that when transmitting recorded material over the Internet it can't be used because naturally the fixed key with the media is not present. In short, received content is not sent over the Internet. But this is about not sending over the Internet because the content is encoded. This is different than talking about keys.

Probably content over the Internet will be locked. But how will that key be processed at the other end? Or if it isn't locked, we absolutely cannot use the Internet. I don't think we've heard anything about these issues.

From this angle, then, the question in the first part that Mr. Shiina and I are most interested in is: "Is this not the same as copy-free?" Looking at our figure at the player in the center, if we copied this content to a different media with a different player, then couldn't we just keep on copying without generation or copy limits because in the red section with IDy, x times y is a lot, right? I don't think we've heard an explanation that addresses this question. I think this is the biggest area of interest.

Shiina (*Study Group member*) — If we talk about the figure, the recorder is there in the top left and below it is something like an optical media drive. As long as you use these, you can keep generating the encryption key for recordings endlessly. And yet it's not written that when you burn something, the key can be generated endlessly. I

completely understand that when it's sent over the Internet the media ID becomes y and you can't play or copy the content. But summing up once again, generation management does not exist, generation restrictions do not exist, and copy limits do not exist. So why on earth is this not called copy-free?

Murai (*Study Group Chair*) — Anyone to address this?

Kacho(Kachô) (*Study Group member*) — Putting it a little more simply, you can't call a technology that doesn't allow the rights holder to select copy-never or copy control a protection technology. Does that sum it up better?

Seki (*Study Group member*) — We've been calling it protection technology or protection, but it's not really. As you said, we are saying protection from a different standpoint. It is not the protection technology we have said here.

Shiina (*Study Group member*) — I don't know who to ask this to, but copy-once and copy-one-generation are different, right. I understand COG is copy-one-generation, but what is "generation" referring to? When you record a broadcast to hard disk is that recording copy-one-generation? Or is it no-more-copies?

Murai (*Study Group Chair*) — Can someone answer this? Perhaps Mr. Tago.

Tago (*Study Group member*) — I'll respond to just the first half.

Putting aside whether this should be named copy-free, EPN does not apply generation restrictions or restrictions on the number of copies. This is a fact. This is what I've said repeatedly. But there are restrictions in place that make this different from analog or terrestrial analog where there are no limits whatsoever. This is that only media, players, and recorders that protect content with encryption as given in the content protection method can use this content. As I've been saying from the beginning, EPN does not place any limits on the number of copies or copy generations or what have you. What this should be called is a separate issue.

That's all.

Shiina (*Study Group member*) — Will you not answer my question?

Tago (*Study Group member*) — About copy-once?

Murai (*Study Group Chair*) — About what section does one generation refer to?

Tago (*Study Group member*) — Mr. Seki would be better to answer about copy-one-generation.

Shiina (*Study Group member*) — The reason why I'm talking about this is that if we say copy-once is useless and we apply something like copy-one-generation, in my understanding, this means the rule allows the user to have one local copy. Nevertheless, the conversation about move failures came up and we got carried away with that, though I think move failures are the responsibility of the manufacturers because the devices do not functional meet their demanded specifications. From there before we suddenly go with EPN, for example — and this isn't a proposal, just a springboard for discussion — one type of operation would attach a copy-one-generation flag to content captured on a hard disk and then allow that content to be copied to optical media, which is the one generation. I think there is room between the approach of our current framework, that is copy-one-generation, and the EPN approach. I think without discussing this and going to copy-free is very unusual.

I have no idea whether the broadcasters' proposal is correct or what is correct, but at the very least what is fixed on the hard disk is the parent copy. If we think of this as the parent copy and then add a copy-one-generation flag to it, then the situation is very similar to one generation when copying an audio CD, and, I think there is some affinity there, we can consider the "between" area.

I think the possibility of move failures alone invalidates copy-once. So, at the very least, how about moving from copy-once to EPN, which I can't help feeling is a great leap.

Murai (*Study Group Chair*) — First, let's split our discussion into two parts for COG and EPN.

Nakajima (*Study Group member*) — That's for me, right? First of all, content broadcast with COG set passes through the tuner of the hard disk and is set to no-more-copies when copied to the hard disk. This is the way it is spelled out in the guidelines. So, beyond this the content cannot be copied. Therefore, it must be moved. This is how it is.

Shiina (*Study Group member*) — I realize that.

Nakajima (*Study Group member*) — Then, if we keep that content set to copy-once by some means and leave the content on the hard disk — and I believe there was some talk of being able to make endless copies if this were the case — then this would mean, from the perspective of manufacturers, that DTCP would have to be used for the internal bus that connects the terrestrial-digital tuner's internal recorder to the built-in hard disk or external hard disk. This would involve changing the guidelines completely and, in reality, it would be impossible or at least very time intensive.

Shiina (*Study Group member*) — What I said was not necessarily a proposal. All I was trying to say was that there are several things between COG and EPN.

Nakajima (*Study Group member*) — If that's true, then we would like the broadcasters to come out with something. At the present time, there are no other alternatives. We can only discuss a world of 0 or 1.

Shiina (*Study Group member*) — One more thing. Something I picked up in your statement was that DTCP is used when connecting to external devices but not used for internal connections. Does this mean it is an original standard?

Nakajima (*Study Group member*) — It is an internal standard.

Shiina (*Study Group member*) — The majority of devices come with hard disks and DVDs.

Nakajima (*Study Group member*) — I'm not sure if a majority do or not.

Shiina (*Study Group member*) — I'm not sure either, but at least when I look around the shops there are plenty of those types of devices. So these devices do not follow DTCP internally?

Nakajima (*Study Group member*) — They conform to Japan's TR-B14 broadcasting format, not DTCP, so there isn't any problem. When the signal is taken externally, the transfer protocol conforms to DTCP.

Fujisawa (*observer from NHK*) — Shuichi Fujisawa from the NHK. I've been listening to the debate so far and I think I should mention a couple of points, if I may.

Can I see the previous page in JEITA's PowerPoint presentation? I think this is a very easy-to-understand reference. On the right side of the slide, it says that defining a new CCI on the upstream side requires changes in the protection method standards on the downstream side. In fact, this works both ways.

One more reference I'd like to look at is one page in Mr. Seki's notes with the title "Transmission Operational Rules (DTCP Encoding Rules)." Here, for example, under free broadcasts with content protection, copy prohibited is marked with an x. So why is this marked as x? Well, in fact, among the broadcasters, there were serious discussions that free broadcasts should be made copy-never operations despite being free broadcasts. But to put it simply, this became x in order to be consistent with the DTCP rules.

Well, why did you decide to do that, you might ask. Let's go back to JEITA's reference again. Here you see a digital receiver. This one receiver is bound by the regulations in the operational guidelines for broadcast signals and is bound by a licensing agreement because it is equipped with DTCP, which is a regulation also. If these two bindings conflict, then there is no way to build the receivers. So this is why the DTCP rules, the transmission operational guidelines, and the TR match up.

Now if there should be some problem in implementation — it's difficult to build to these guidelines — for sure we would have heard from the manufacturers that this cannot be built. If this were the case, we would have never ended up with

this TR. What I want you to understand is that devices have been built to these guidelines.

Murai (*Study Group Chair*) — I apologize for the confusing debate session today. I was a bit inept in leading our meeting this time. I'll have to restrain my desire to summarize our technical issues. We had presentations from the manufacturers' side and the broadcasters' side at our meeting today. Less than the Dharma that appeared in the manufacturers' presentation, my impression is one of the three wise monkeys, so I think it was good to have as much frank talk as possible. Through today's discussions I think a number of things have become clear such as the relationship between COG copy-once and the DTCP rules after content is placed on a hard disk and, concerning the move function, the relationship between a number of restrictions determined by TR-B14 and the issues in the move function, which has become a topic. In particular, we had had explanations describing B-CAS enforcement and the relationship between scrambling and B-CAS to ensure devices function properly, but even after one explanation there were still difficult points remaining. Today, we have reached the end of that discussion. As I said at the beginning, we plan on taking two meetings to reach a common understanding of the relevant technologies. I expect the Secretariat will be urgently organizing the present state of our discussions so that at our next meeting on the 27th we will have people who can answer or address the points and left-off issues from today's discussions, have new observers attend to give extra explanations, and have the Secretariat explain anything they might be able to research. In addition, I too will make an effort to examine how I can proceed with our operations on the 27th more efficiently.

At the meeting on the 27th, I hope that in general we can examine as thoroughly as possible the various issues that have emerged in past meetings as well as the questions, reports, and other details about conditions overseas.

As we did today with submitting questions in advance and arranging them before the meeting, for more efficient discussions at the next meeting as well, please bring matters you want to ask about, requests about points you want to discuss thoroughly, or that you want to hear from a certain individual, and any other opinions to the Secretariat.

Because this Study Group's time is limited, I hope that we can arrange matters as much as possible beforehand and that members can make their discussions as compact as possible. I too will be making a number of adjustments in advance of the next meeting.

One more point. There have been some changes to the schedule announced last time. So I would ask for your cooperation.

Do you have anything to add from the Secretariat?

Ogasawara (*Secretary and Head of the Content Distribution Promotion Office*) — As the Chair has just said, there have been some urgent changes to the examination schedule in Reference 3. After confirming everyone's availability with the original schedule, I have decided to make the sixth meeting, the one after the fifth meeting on November 27th, on December 7th. The seventh meeting is a spare meeting, and the eighth meeting will be changed in the same way as we have done up to now.

The next meeting on November 27th, next Monday, will begin at 10:30 in the morning at the Mita Kaigisho.

The following meeting on December 7th will be in the evening, I'm afraid, starting from 7 p.m. I apologize for booking an evening session. This meeting is scheduled to be held in a conference room at MIC.

Murai (*Study Group Chair*) — Thank you very much, everyone. This adjourns today's meeting.