The Act on Communications Interception for Criminal Investigation is hereby promulgated.

Act on Communications Interception for Criminal Investigation

(Act No. 137 of August 18, 1999)

Table of Contents

Chapter I General Provisions

(Purpose)

Article 1 In light of the fact that organized crimes are extremely harmful to a peaceful and sound social life, and taking into account the circumstances where in an increasing number of serious criminal cases, such as organized homicides committed in conspiracy by multiple persons and offenses relating to illegal trading of drugs and firearms, it is extremely difficult to clarify the factual background of the case unless telephone calls or other telecommunications used for mutual contact among criminals are intercepted, the purpose of this Act is to specify requirements, procedures and other necessary matters concerning compulsory measures for the interception of telecommunications prescribed in the Code of Criminal Procedure (Act No. 131 of 1948) necessary for duly tackling the circumstances, with the aim of contributing to correct clarification of the factual background of respective cases without unduly violating the secrecy of communications.

(Definitions)

Article 2 (1) The term "communications" as used in this Act means telephone calls or other telecommunications whose transmission line is in whole or in part wired (excluding wire attached to electrical facilities for the purpose of sending or receiving radio waves or other electromagnetic waves by a system other than a wired system) or whose transmission line is equipped with

switching facilities.

(2) The term "interception" as used in this Act means to receive communications being transmitted between third parties in order to know the content thereof without obtaining consent from any of the parties using those communications.

(3) The term "carrier, etc." as used in this Act means a person who engages in a business to intermediate third parties' communications by using facilities for telecommunications (hereinafter referred to as "telecommunications facilities") or otherwise provide telecommunications facilities for third parties' communications, and any other person who has installed telecommunications facilities that can intermediate communications among many or unspecified persons for the purpose of their own business.

(4) The term "encryption" as used in this Act means to conduct conversion of signals transmitting the content of the communications, signals transmitting information on the dates and times of transmissions, or other signals that are provided for use in information processing by computers (hereinafter referred to as the "original signals") by the use of computer and conversion codes (meaning codes for converting signals; the same applies hereinafter), thereby making it impossible to restore the original signals to their original state without the use of conversion codes corresponding to the conversion codes used for that conversion process (hereinafter referred to as "corresponding conversion codes"), and the term "decryption" as used in this Act means to restore signals made through encryption (hereinafter referred to as "encrypted signals") to the state of the original signals through conversion process using a computer and corresponding conversion codes.

(5) The term "temporary storage" as used in this Act means to temporarily record and store encrypted signals in a recording medium only for the period until the decryption thereof is conducted.

(6) The term "reproduction" as used in this Act means to process communications restored through decryption of encrypted signals (limited to those pertaining to signals transmitting the content of the communications) that were temporarily stored using a computer, into a state perceptible through the human sense of hearing or sense of sight by a method of play of sound, display of characters, or other method.

Chapter II Requirements and Procedures for Communications Interception

(Warrants for Interception)

Article 3 (1) In cases falling under any of the following items, when there is a circumstance sufficient to suspect the possibility that communications concerning plotting, instructions, or other mutual contact in relation to the commission of, preparation for or subsequent measures such as suppression of

evidence pertaining to any of the crimes prescribed in the following items (for items (ii) and (iii), a series of the crimes), or other matters in relation to commission of the relevant crime (hereinafter referred to as "crime-related communications" in this paragraph) may take place and when it is extremely difficult to identify criminals or clarify the status or content of the offense by other means, a public prosecutor or judicial police officer may, with a warrant for interception issued by a judge, intercept crime-related communications conducted by the use of a means of communication identified with telephone numbers or other numbers or codes for distinguishing senders or addressees (hereinafter referred to as "telephone numbers, etc.") (hereinafter a means of communication thus identified is referred to as a "means of communication") that the suspect uses under a contract with a carrier, etc. (excluding a means of communication that is found to be unlikely to be used by criminals for crime-related communications) or a means of communication that is sufficiently suspected to be used by criminals for crime-related communications:

(i) the case where there are sufficient grounds to suspect that any of the crimes set forth in Appended Table 1 or Appended Table 2 has been committed and when there is a circumstance sufficient to suspect that it has been conspired by multiple persons (for crimes set forth in Appended Table 2, limited to the crime where acts consisting the crime are committed by a group of persons who act in accordance with the division of roles assigned in advance; the same applies in the following item and item (iii));

(ii) the case where there are sufficient grounds to suspect that any of the crimes set forth in Appended Table 1 or Appended Table 2 has been committed and any of the following crimes will be subsequently committed and when there is a circumstance sufficient to suspect that it has been conspired by multiple persons regarding these crimes:

(a) any of the crimes set forth in Appended Table 1 or Appended Table 2 of the same or similar type as the relevant crime that will be committed in the same or similar manners as the relevant crime;

(b) any of the crimes set forth in Appended Table 1 or Appended Table 2 that will be committed based on a plan of a series of offenses including the commission of the relevant crime; or

(iii) the case where there are sufficient grounds to suspect that a crime punishable with death penalty, life imprisonment, imprisonment or imprisonment without work for a long term of not less than two years has been committed inseparably with any of the crimes set forth in Appended Table 1 or Appended Table 2 for the preparation necessary for the commission of the latter crime and that the relevant crime set forth in Appended Table 1 or Appended Table 2 will be subsequently committed, and when there are sufficient reasons to suspect that it has been conspired by

multiple persons.

(2) With regard to crimes set forth in Appended Table 1 for which acts of transfer, acceptance, lending, borrowing or delivery are to be punished, the existence of a circumstance sufficient to suspect a conspiracy by multiple persons is not required, notwithstanding the provisions of the preceding paragraph.

(3) Interception under the provisions of the preceding two paragraphs cannot be conducted at a person's dwelling or in a residence, building, or vessel that a person watches over, except for the case where it is conducted at a place that a carrier, etc. watches over; provided, however, that this does not apply when consent is obtained from the owner of the dwelling, the person who watches over the relevant place or the deputy thereof.

(Procedures for Request for a Warrant)

Article 4 (1) A request for a warrant for interception must be filed by a public prosecutor (limited to a prosecutor designated by the Prosecutor General; hereinafter the same applies in this Article and Article 7) or a judicial police officer (limited to a police officer in the rank of superintendent or higher designated by the National Public Safety Commission or a Prefectural Public Safety Commission, a ministry narcotics agent designated by the Minister of Health, Labour and Welfare, or a coast guard officer designated by the Commandant of the Japan Coast Guard; hereinafter the same applies in this Article and Article 7) with a judge of a district court.

(2) When filing a request referred to in the preceding paragraph, if any request for a warrant targeting the same means of communication has previously been filed or the warrant has previously been issued with regard to the alleged facts that are the same in whole or in part as the alleged facts for which the relevant request is to be filed, a public prosecutor or judicial police officer must inform a judge of that fact.

(3) A request for permission referred to in Article 20, paragraph (1) or permission referred to in Article 23, paragraph (1) must be filed by a public prosecutor or judicial police officer when filing a request referred to in paragraph (1).

(Issuance of a Warrant for Interception)

Article 5 (1) When a judge who has received a request referred to in paragraph (1) of the preceding Article finds that there are grounds for the request, the judge is to specify a period not exceeding ten days as a period during which interception is authorized and issue a warrant for interception.

(2) When issuing a warrant for interception, a judge may set conditions that the judge finds appropriate with regard to the implementation of interception (meaning to intercept communications and to monitor the status of communications in a manner that enables immediate interception regarding a

means of communication; the same applies hereinafter).
(3) When a request referred to in paragraph (3) of the preceding Article has been filed and when a judge finds it appropriate, the judge is to grant permission for the request.
(4) When a judge grants the permission referred to in Article 20, paragraph (1) under the provisions of the preceding paragraph, the judge must specify a place managed by a communication manager, etc. (meaning a person who manages the part of a means of communication with which the implementation of interception is conducted (for a company or other corporation or an association, its officer or employee) or the deputy thereof; the same applies hereinafter) as the place of the implementation of interception. In this case, when a person who filed a request referred to in paragraph (3) of the preceding Article has filed an application, and a judge finds it appropriate in consideration of the situation of the place of the implementation on interception pertaining to the application and other circumstances, the judge is to specify the place of the implementation of interception during the designated period (meaning the designated period prescribed in Article 20, paragraph (1); hereinafter the same applies in this paragraph) and the place of implementation of interception during a period other than the designated period, respectively.

(Matters to Be Stated in a Warrant for Interception)
Article 6 (1) A warrant for interception must contain the name of the suspect, a summary of the alleged facts, the name of the offense, the applicable penal statute, communications to be intercepted, the means of communication subject to the implementation of interception, the method and place of the implementation of interception, the period during which interception is authorized, conditions concerning the implementation of interception, the validity period and the fact that dispositions of interception may not be commenced after the lapse of that validity period and the warrant for interception must be returned, the date of the issuance, and other matters specified by Rules of the Supreme Court, and a judge must affix their signature and seal thereon; provided, however, that if the suspect's name is not known, it suffices to state to that effect in lieu of the name.
(2) When a judge grants the permission referred to in Article 20, paragraph (1) or the permission referred to in Article 23, paragraph (1) under the provisions of paragraph (3) of the preceding Article, the judge is to state to that effect in a warrant for interception.

(Extension of the Period during Which Interception is Authorized)
Article 7 (1) When a judge of a district court finds it necessary, the judge may extend the period during which interception is authorized by specifying a

period not exceeding ten days upon a request by a public prosecutor or judicial police officer; provided, however, that the period during which interception is authorized must not exceed 30 days in total.

(2) The extension of the period referred to in the preceding paragraph must be made by stating the period to be extended and the grounds therefor in a warrant for interception, to which the relevant judge affixes their signature and seal.

(Issuance of a Warrant for Interception Concerning the Same Facts)

Article 8 In the case where a request for a warrant for interception has been filed and when the alleged facts pertaining to the request contain the same alleged facts for another warrant for interception issued in the past, a judge may issue a warrant for interception of the same means of communication only when the judge finds that there are special circumstances that require further interception thereof.

(Creation of Conversion Codes and Corresponding Conversion Codes)

Article 9 In cases set forth in the following items, court clerks and other court officials are to take measure specified respectively therein, as ordered by a judge:

(i) when a warrant for interception contains the statement to the effect that the permission referred to in Article 20, paragraph (1) is granted: create conversion codes to be used for encryption under the provisions of that paragraph and their corresponding conversion codes, and provide them to the communication manager, etc.;

(ii) when a warrant for interception contains the statement to the effect that the permission referred to in Article 23, paragraph (1) is granted: measures set forth in (a) through (c) below:

(a) create conversion codes to be used for encryption under the provisions of Article 23, paragraph (1), and provide them to the communication manager, etc.;

(b) create corresponding conversion codes for the conversion codes referred to in (a) and conversion codes to be used for encryption under the provisions of Article 26, paragraph (1), and take technical measures to make them unavailable except for the specified computer (meaning the specified computer prescribed in Article 23, paragraph (2)) designated to be used by the public prosecutor or judicial police officer for the implementation of interception, and provide those codes to the public prosecutor or judicial police officer; or

(c) create corresponding conversion codes for the conversion codes provided to the public prosecutor or judicial police officer referred to in (b) above, and

keep them.

(Presentation of a Warrant for Interception)

Article 10 (1) A warrant for interception must be presented to a communication manager, etc.; provided, however, that this does not apply to a summary of the alleged facts.

(2) The provisions of the preceding paragraph also apply when the period during which interception is authorized has been extended.

(Necessary Measures)

Article 11 (1) With regard to the implementation of interception, it is permitted to connect equipment for interception to telecommunication facilities or to take any measures necessary for the implementation of interception.

(2) A public prosecutor or judicial police officer may have public prosecutor's assistant officers or judicial police officials take the measures referred to in the preceding paragraph.

(Duty of Cooperation of Carriers)

Article 12 A public prosecutor or judicial police officer may ask a carrier etc. for necessary cooperation for the implementation of interception, such as the connection of equipment for interception. In this case, the carrier, etc. must not refuse it without justifiable grounds.

(Attendance)

Article 13 (1) When conducting the implementation of interception, attendance of a communication manager, etc. is required. When a communication manager, etc. cannot attend, a public prosecutor or judicial police officer must have an employee of a local government attend the implementation of interception.

(2) An observer may present their opinions concerning the implementation of interception to a public prosecutor or judicial police officer.

(Interception for the Purpose of Judging the Relevance)

Article 14 (1) With regard to communications that took place during the implementation of interception but for which it is not clear whether they fall under the communications to be intercepted as stated in a warrant for interception (hereinafter simply referred to as the "communications to be intercepted"), a public prosecutor or judicial police officer may intercept those communications only to the minimum extent necessary for judging whether they fall under the communications to be intercepted.

(2) With regard to communications in a foreign language or communications using ciphers or other method that makes it impossible to instantly restore the

content thereof, for which it is impossible to make a judgment as to whether they fall under the communications to be intercepted as it is difficult to know the content thereof at the time of interception, a public prosecutor or judicial police officer may intercept those communications in full. In this case, a judgment as to whether they fall under the communications to be intercepted must be made promptly thereafter.

(Interception of Communications Concerning the Commission of Another Crime)

Article 15 While conducting the implementation of interception, if there are communications whose content is evidently found to be the fact that any crime other than the crime stated as the alleged facts in a warrant for interception, which is set forth in Appended Table 1 or Appended Table 2 or which is punishable by the death penalty, life imprisonment, imprisonment or imprisonment without work for a minimum period not less than one year, has been committed, is being committed, or is to be committed, a public prosecutor or judicial police officer may intercept those communications.

(Prohibition of Interception of Communications Related to Services of Physicians)

Article 16 With regard to communications with a physician, dentist, midwife, nurse, attorney (including a registered foreign lawyer), patent attorney, notary public or a person engaged in a religious occupation (excluding a person stated as the suspect in a warrant for interception), when they are found to be related to those persons' services provided upon a request of a third party, they must not be intercepted.

(Search of Telephone Numbers of the Other Parties)

Article 17 (1) With regard to communications that took place during the implementation of interception, when the communications fall under communications to be intercepted or communications for which interception is authorized under the provisions of Article 15, or when it is found that it will contribute to making a judgment as to whether they fall under the communications to be intercepted under the provisions of Article 14, a public prosecutor or judicial police officer may search the telephone numbers, etc. of the other parties to the communications at the place of the implementation of interception. In this case, it is not necessary to obtain a warrant separately.

(2) A public prosecutor or judicial police officer may ask a carrier, etc. for necessary cooperation in relation to the dispositions referred to in the preceding paragraph. In this case, the carrier, etc. must not refuse it without justifiable grounds.

(3) When it is necessary to take measures for the search referred to in paragraph (1) at a place other than the place of the implementation of interception, a public prosecutor or judicial police officer may request a carrier, etc. that can take those measures to take them after informing the carrier, etc. of the fact that it is a search to be conducted under the provisions of that paragraph. In this case, the provisions of the second sentence of the preceding paragraph apply mutatis mutandis.

(Measures When the Implementation of Interception is to Be Suspended or Terminated)

Article 18 When communications are taking place at the time when the implementation of interception is to be suspended or terminated as stated in a warrant for interception, it is permitted to continue the implementation of interception until the use of the relevant means of communication (hereinafter referred to as "conversations") is terminated.

(Termination of the Implementation of Interception)

Article 19 When the grounds or necessity for interception have ceased to exist, the implementation of interception must be terminated even during the period during which interception is authorized as stated in a warrant for interception.

(Procedures for Communications Interception by Ordering Temporary Storage)

Article 20 (1) A public prosecutor or judicial police officer may, upon the permission of a judge, intercept all communications that take place during the period designated by a public prosecutor or judicial police officer within the period during which interception is authorized as stated in a warrant for interception (excluding the period after the termination of the implementation of interception under the provisions of the preceding Article) (when, at the end of the period thus designated, the implementation of interception may be continued under the provisions of Article 18, including the relevant period during which interception may be continued; hereinafter the period thus designated is referred to as the "designated period") by means of ordering a communication manager, etc. to encrypt the original signals (limited to signals transmitting the content of the communications) by using conversion codes provided under the provisions of Article 9, item (i) and to temporarily store the encrypted signals made through the encryption. With regard to the implementation of interception in this case, the provisions of Article 13 do not apply.

(2) When conducting interception under the provisions of the preceding paragraph, a public prosecutor or judicial police officer is to order a communication manager, etc. to encrypt the original signals transmitting the

information on the dates and times of commencement and termination of conversations during the designated period by using conversion codes prescribed in that paragraph and to temporarily store the encrypted signals made through the encryption.

(3) When conducting interception under the provisions of paragraph (1), a public prosecutor or judicial police officer may ask a communication manager, etc. to store information of telephone numbers, etc. of the other parties to the communications subject to interception under the provisions of paragraph (1) until the procedures referred to in paragraph (7) of the following Article are completed for the purpose of using them for the procedures referred to in that paragraph. In this case, the provisions of the second sentence of Article 17, paragraph (2) apply mutatis mutandis.

(4) When a communication manager, etc. cannot store information of the telephone numbers, etc. referred to in the preceding paragraph, a public prosecutor or judicial police officer may request a carrier, etc. that can store the information to store the information until the procedures referred to in paragraph (7) of the following Article are completed after informing the carrier, etc. of the fact that the request is made for the purpose of using the information for the procedures referred to in that paragraph. In this case, the provisions of the second sentence of Article 17, paragraph (3) apply mutatis mutandis.

(5) A public prosecutor and judicial police officer must not enter the place of implementation of interception during the designated period.

(6) A public prosecutor and judicial police officer may not conduct the implementation of interception except by the method prescribed in paragraph (1) during the designated period.

(7) The restoration of the communications intercepted under the provisions of paragraph (1) through decryption must not be conducted except for cases prescribed in paragraph (1) of the following Article.

Article 21 (1) When having conducted interception under the provisions of paragraph (1) of the preceding Article, a public prosecutor or judicial police officer may order a communication manager, etc. to decrypt encrypted signals that are temporarily stored under the provisions of that paragraph by using corresponding conversion codes provided under the provisions of Article 9, item (i), and thereby restore the communications intercepted under the provisions of that paragraph, and simultaneously reproduce the restored communications as prescribed in paragraphs (3) through (6) at the place of the implementation of interception (when the place of the implementation of interception during a period other than the designated period has been specified, at that place). With regard to the implementation of reproduction (meaning to reproduce

communications, to confirm the status of temporal storage in a manner to enable instant reproduction with regard to the recording medium used for the temporal storage, and to decrypt encrypted signals; the same applies hereinafter) in this case, the provisions of Articles 11 through 13 apply mutatis mutandis.

(2) When conducting the implementation of reproduction under the provisions of the preceding paragraph, a public prosecutor or judicial police officer is to order a communication manager, etc. to decrypt encrypted signals that are temporarily stored under the provisions of paragraph (2) of the preceding Article by using corresponding conversion codes prescribed in the preceding paragraph, and thereby to restore the original signals transmitting the information on the dates and times of commencement and termination of conversations encrypted under the provisions of paragraph (2) of the preceding Article.

(3) Out of the restored communications through decryption under the provisions of paragraph (1), a public prosecutor or judicial police officer may reproduce communications falling under communications to be intercepted and may also reproduce communications for which it is not clear whether they fall under the communications to be intercepted only to the minimum extent necessary for judging whether they fall under the communications to be intercepted.

(4) Out of the communications restored through decryption under the provisions of paragraph (1), a public prosecutor or judicial police officer may reproduce all of the communications for which it is impossible to make a judgment as to whether they fall under the communications to be intercepted as it is difficult to know the content thereof at the time of reproduction, because they are in a foreign language or use ciphers or other methods that make it impossible to instantly restore the content thereof. In this case, a judgment as to whether they fall under the communications to be intercepted must be made promptly thereafter.

(5) When the restored communications through decryption under the provisions of paragraph (1) contain the communications prescribed in Article 15, a public prosecutor or judicial police officer may reproduce those communications.

(6) The provisions of Article 16 apply mutatis mutandis to the case where the restored communications through decryption under the provisions of paragraph (1) are reproduced.

(7) With regard to communications intercepted under the provisions of paragraph (1) of the preceding Article, when they fall under communications to be intercepted or communications that may be reproduced under the provisions of paragraph (5), or when it is found that it will contribute to making a judgment as to whether they fall under the communications to be intercepted under the provisions of paragraph (3) or (4), a public prosecutor or judicial police officer

may receive disclosure of the telephone numbers, etc. of the other parties to the relevant communications out of the telephone numbers, etc. whose storage has been asked for under the provisions of paragraph (3) of that Article or has been requested under the provisions of paragraph (4) of that Article. In this case, the provisions of the second sentence of Article 17, paragraph (1) apply mutatis mutandis.

(8) When the implementation of reproduction under the provisions of paragraph (1) has not been terminated within the period during which interception is authorized as stated in a warrant for interception, it must be terminated as promptly as possible after the end of the period during which interception is authorized as stated in the warrant for interception.

(9) When the grounds or necessity for interception have ceased to exist, even during the period during which interception is authorized as stated in a warrant for interception, the implementation of reproduction under the provisions of paragraph (1) must not be commenced if it has yet to be commenced and must be terminated if it has been commenced; provided, however, that the implementation of reproduction may be conducted with regard to the encrypted signals that have temporarily been stored by the time when the grounds or necessity for interception cease to exist, only in the case where the grounds or necessity for interception have ceased to exist due to the facts that a circumstance sufficient to suspect that communications falling under communications to be intercepted will take place has ceased to exist, that the means of communication subject to the implementation of interception as stated in the warrant for interception has ceased to be the one used by the suspect under a contract with a carrier, etc., or the one sufficiently suspected to be used for communications by criminals falling under communications to be intercepted.

Article 22 (1) When decryption under the provisions of paragraph (1) of the preceding Article is completed, a communication manager, etc. must immediately delete all of the encrypted signals temporarily stored under the provisions of Article 20, paragraph (1). The same applies to the encrypted signals temporarily stored under the provisions of Article 20, paragraph (2) in the case where decryption under the provisions of paragraph (2) of the preceding Article is completed.

(2) When the implementation of reproduction under the provisions of paragraph (1) of the preceding Article is terminated or the commencement of the implementation of reproduction has come to be prohibited under the provisions of paragraph (9) of that Article, if there are any encrypted signals temporarily stored under the provisions of Article 20, paragraphs (1) and (2) that have yet to be decrypted under the provisions of paragraphs (1) and (2) of the preceding

Article, a public prosecutor or judicial police officer must immediately order a communication manager, etc. to delete all those encrypted signals.

(Procedures for Communications Interception Using Specified Computers)

Article 23 (1) A public prosecutor or judicial police officer may, upon the permission of a judge, order a communication manager, etc. to encrypt the original signals (limited to signals transmitting the content of the communications) by using conversion codes provided under the provisions of Article 9, item (ii), (a) with regard to all communications that take place during the implementation of interception, and to transmit the encrypted signals made through the encryption to a specified computer installed at the place of the implementation of interception, and thereby intercept those communications in any of the following manners. With regard to the implementation of interception in this case, the provisions of Article 13 do not apply, and with regard to interception under the provisions of item (ii), the provisions of Article 20, paragraphs (3) and (4) apply mutatis mutandis:

(i) decrypt encrypted signals, simultaneously upon receiving them, by using corresponding conversion codes provided under the provisions of Article 9, item (ii), (b), and intercept the restored communications as prescribed in Articles 3 and 14 through 16; or

(ii) intercept the communications whose content is transmitted by the use of the original signals for the encrypted signals by temporarily storing encrypted signals, simultaneously upon receiving them.

(2) The specified computer prescribed in the preceding paragraph means a computer that has all of the following functions:

(i) a function to temporarily store encrypted signals that have been transmitted;

(ii) a function to decrypt encrypted signals that have been transmitted;

(iii) a function to automatically encrypt and record in a recording medium all of the communications intercepted under the provisions of item (i) of the preceding paragraph upon interception thereof, or all of the communications reproduced under the provisions of paragraph (4) upon reproduction thereof;

(iv) a function to create the original signals that transmit information on the dates and times of commencement and termination of conversations that took place during the implementation of interception, the dates and times of commencement and termination of communications intercepted under the provisions of item (i) of the preceding paragraph, the dates and times of commencement and termination of communications reproduced under the provisions of paragraph (4), and other matters specified by Cabinet Order, and to automatically encrypt and record those original signals in a recording medium referred to in the preceding item;

(v) a function to record the communications referred to in item (iii) and the original signals referred to in the preceding item that are recorded in a recording medium referred to in item (iii) in another recording medium without encrypting them, simultaneously upon recording them in the recording medium referred to in item (iii) through the functions referred to in the preceding two items;

(vi) a function to prevent the corresponding conversion codes that have been inputted (limited to corresponding conversion codes provided under the provisions of Article 9, item (ii), (b)) from being used for processing other than decryption prescribed in item (ii);

(vii) a function to prevent the conversion codes that have been inputted (limited to conversion codes provided under the provisions of Article 9, item (ii), (b)) from being used for processing other than encryption prescribed in items (iii) and (iv); and

(viii) a function to automatically delete all of the encrypted signals temporarily stored as prescribed in item (i) at the time of decrypting them as prescribed in item (ii).

(3) When a warrant for interception contains the statement to the effect that the permission referred to in paragraph (1) is granted, a public prosecutor and judicial police officer cannot conduct the implementation of interception except by the method prescribed in that paragraph.

(4) When having conducted interception under the provisions of paragraph (1), item (ii), a public prosecutor or judicial police officer may restore communications intercepted under the provisions of paragraph (1), item (ii) by decrypting encrypted signals temporarily stored under the provisions of that item by using a specified computer (meaning the specified computer prescribed in paragraph (2); the same applies in paragraph (6) and Article 26, paragraph (1)) and by using corresponding conversion codes provided under the provisions of Article 9, item (ii), (b), and may simultaneously reproduce the restored communications in accordance with the provisions of Article 21, paragraphs (3) through (6), at the place of the implementation of interception. With regard to the implementation of reproduction in this case, the provisions of Articles 11 and 12 and Article 21, paragraphs (7) through (9) apply mutatis mutandis.

(5) The restoration of communications intercepted under the provisions of paragraph (1), item (ii) through decryption must not be conducted except for the case under the provisions of the preceding paragraph.

(6) With regard to encrypted signals temporarily stored under the provisions of paragraph (1), item (ii), if there are any encrypted signals, other than those automatically deleted with a function of a specified computer, that have not been decrypted under the provisions of paragraph (4) at the time when the implementation of reproduction under the provisions of that paragraph is

terminated or when the commencement of the implementation of reproduction has come to be prohibited under the provisions of Article 21, paragraph (9) as applied mutatis mutandis pursuant to paragraph (4), a public prosecutor or judicial police officer must immediately delete all of those encrypted signals.

Chapter III Recording of Communications Interception

(Recording of Intercepted Communications)

Article 24 (1) Intercepted communications (in the case of the interception under the provisions of Article 20, paragraph (1), communications reproduced under the provisions of Article 21, paragraph (1)) must all be recorded in a recording medium using an audio recording or any other appropriate method in accordance with the nature of communications. In this case, it is permitted to simultaneously record them in another recording medium by the same method for the purpose of using them for the procedures referred to in Article 29, paragraph (3) or (4).

(2) When the implementation of interception (in the case of the implementation of interception under the provisions of Article 20, paragraph (1), the implementation of reproduction under the provisions of Article 21, paragraph (1)) is suspended or terminated, recording in the recording medium being used at that time must be terminated.

(Seal of a Recording Medium)

Article 25 (1) When the implementation of interception has been suspended or terminated, an observer must be asked to promptly seal the recording medium (excluding the recording medium prescribed in the following paragraph) in which recording has been made under the provisions of the first sentence of paragraph (1) of the preceding Article. The same applies when a recording medium is replaced during the implementation of interception or otherwise recording in a recording medium has been terminated.

(2) With regard to a recording medium in which communications reproduced under the provisions of Article 21, paragraph (1) have been recorded under the provisions of the first sentence of paragraph (1) of the preceding Article, an observer must be asked to promptly seal it when the implementation of reproduction has been suspended or terminated. The same applies when a recording medium is replaced during the implementation of reproduction or otherwise recording in a recording medium has been terminated.

(3) With regard to the recording media referred to in the preceding two paragraphs, their copies may be made for the purpose of using them for the procedures referred to in Article 29, paragraph (3) or (4) before asking an observer to seal them, except for a case where there are any recording media in

which recording has been made under the provisions of the second sentence of paragraph (1) of the preceding Article.

(4) A recording medium sealed by an observer must be submitted to a judge of a court to which the judge who issued the relevant warrant for interception belongs, without delay.

(Recording of Communications Interception Using a Specified Computer)

Article 26 (1) Notwithstanding the provisions of the preceding two Articles, when having conducted interception under the provisions of Article 23, paragraph (1), all of the intercepted communications (in the case of the interception under the provisions of item (ii) of that paragraph, communications reproduced under the provisions of Article 23, paragraph (4); hereinafter the same applies in this paragraph and the following paragraph) must be encrypted and recorded in a recording medium, and also the dates and times of commencement and termination of conversations that took place during the implementation of interception, the dates and times of commencement and termination of intercepted communications, and other particulars specified by Cabinet Order must be encrypted and recorded in the relevant recording medium, by using a specified computer and conversion codes provided under the provisions of Article 9, item (ii), (b).

(2) In the case referred to in the preceding paragraph, the intercepted communications and the particulars prescribed in the preceding paragraph are to be all recorded in another recording medium simultaneously for the purpose of using them for the procedures referred to in Article 29, paragraph (3) or (4).

(3) When the implementation of interception under the provisions of Article 23, paragraph (1) (in the case of the implementation of interception under the provisions of item (ii) of that paragraph, the implementation of reproduction under the provisions of paragraph (4) of that Article) is suspended or terminated, recording in the recording medium being used at that time must be terminated.

(4) A recording medium in which recording has been made under the provisions of paragraph (1) must be submitted to the judge prescribed in paragraph (4) of the preceding Article without delay after the termination of the implementation of interception (when there are any encrypted signals temporarily stored under the provisions of Article 23, paragraph (1), item (ii) that have not been decrypted under the provisions of paragraph (4) of that Article at the time of terminating the implementation of interception, after the termination of the implementation of reproduction).

(Submission of a Document Stating the Status of the Implementation of Interception)

Article 27 (1) A public prosecutor or judicial police officer must submit a document stating the following particulars to the judge prescribed in Article 25, paragraph (4) without delay after the termination of the implementation of interception. The same applies when a public prosecutor or judicial police officer files a request for the extension of the period during which interception is authorized under the provisions of Article 7:

(i) the date and time of commencement, any suspension, and termination of the implementation of interception;

(ii) the name and occupation of an observer under the provisions of Article 13, paragraph (1);

(iii) opinions presented by the observer under the provisions of Article 13, paragraph (2);

(iv) the date and time of commencement and termination of conversations that took place during the implementation of interception;

(v) with regard to intercepted communications, provisions that served as the basis for the interception, the date and time of commencement and termination of the intercepted communication, and the names and other particulars that contribute to identification of the parties to the communications;

(vi) with regard to the communications prescribed in Article 15, the name of the offense relating to the communications and the applicable penal statute, as well as the reason for finding that the communications fall under the communications prescribed in that Article;

(vii) the date and time of any replacement of the recording medium during the implementation of interception;

(viii) the date and time when the recording medium was sealed under the provisions of Article 25, paragraph (1) and the name of the observer who sealed the recording medium; and

(ix) other particulars specified by Rules of the Supreme Court with regard to the circumstances of the implementation of interception.

(2) Notwithstanding the provisions of the preceding paragraph, when a public prosecutor or judicial police officer has conducted the implementation of interception under the provisions of Article 23, paragraph (1), item (i), the public prosecutor or judicial police officer must submit a document stating the following matters to the judge prescribed in Article 25, paragraph (4) without delay after the termination of the implementation of interception. The same applies when a public prosecutor or judicial police officer files a request for the extension of the period during which interception is authorized under the provisions of Article 7 after conducting the implementation of interception under the provisions of that item:

(i) the date and time of commencement, any suspension, and termination of the

implementation of interception under the provisions of Article 23, paragraph (1), item (i);

(ii) the date and time of commencement and termination of conversations that took place during the implementation of interception under the provisions of Article 23, paragraph (1), item (i);

(iii) with regard to communications intercepted under the provisions of Article 23, paragraph (1), item (i), provisions that served as the basis for the interception, the date and time of commencement and termination of the intercepted communication, and the names and other particulars that contribute to identification of the parties to the communications;

(iv) with regard to the communications prescribed in Article 15, the name of the offense relating to the communications and the applicable penal statute, as well as the reason for finding that the communications fall under the communications prescribed in that Article;

(v) the date and time of any replacement of the recording medium during the implementation of interception; and

(vi) beyond what is set forth in the preceding items, the particulars specified by Rules of the Supreme Court with regard to the circumstances of the implementation of interception under the provisions of Article 23, paragraph (1), item (i).

(3) A judge who has received a document submitted as prescribed in the preceding two paragraphs is to examine whether the communications referred to in paragraph (1), item (vi) or item (iv) of the preceding paragraph fall under the communications prescribed in Article 15, and when the judge finds that they do not fall under the communications prescribed in Article 15, the judge is to revoke the dispositions of interception of the relevant communications. In this case, the provisions of Article 33, paragraphs (3), (5) and (6) apply mutatis mutandis.

Article 28 (1) Notwithstanding the provisions of paragraph (1) of the preceding Article, if the period of conducting the implementation of interception contains a period during which the implementation of interception under the provisions of Article 20, paragraph (1) was conducted, a public prosecutor or judicial police officer must submit to the judge prescribed in Article 25, paragraph (4) a document stating the particulars set forth in the items of paragraph (1) of the preceding Article for a period other than the relevant period and the following particulars for the period during which the implementation of interception under the provisions of Article 20, paragraph (1) was conducted, respectively, without delay after the termination of the implementation of interception (when there are any encrypted signals temporarily stored under the provisions of Article 20, paragraph (1) that have not been decrypted under the provisions

of Article 21, paragraph (1) at the time of terminating the implementation of interception, after the termination of the implementation of reproduction). The same applies when a public prosecutor or judicial police officer files a request for the extension of the period during which interception is authorized under the provisions of Article 7 after conducting interception under the provisions of Article 20, paragraph (1):

(i) the date and time of commencement and termination of the designated period;

(ii) the date and time of commencement, any suspension, and termination of the implementation of interception under the provisions of Article 20, paragraph (1);

(iii) the date and time of commencement and termination of conversations that took place during the implementation of interception under the provisions of Article 20, paragraph (1);

(iv) the date and time of commencement, any suspension, and termination of the implementation of reproduction under the provisions of Article 21, paragraph (1);

(v) the name and occupation of the observer under the provisions of Article 13, paragraph (1) as applied mutatis mutandis pursuant to Article 21, paragraph (1);

(vi) opinions presented by the observer under the provisions of Article 13, paragraph (2) as applied mutatis mutandis pursuant to Article 21, paragraph (1);

(vii) particulars sufficient to identify the parts of the conversations prescribed in item (iii) that respectively correspond to encrypted signals that have been decrypted under the provisions of Article 21, paragraph (1), encrypted signals which were deleted before the decryption under the provisions of that paragraph, and any other encrypted signals;

(viii) with regard to communications reproduced under the provisions of Article 21, paragraph (1), the provisions that served as the basis for the reproduction, the date and time of commencement and termination of the reproduced communication, and the names and other particulars that contribute to identification of the parties to the communications;

(ix) with regard to the communications prescribed in Article 15, the name of the offense relating to the communications and the applicable penal statute, as well as the reason for finding that the communications fall under the communications prescribed in that Article;

(x) the date and time of any replacement of the recording medium during the implementation of reproduction;

(xi) the date and time when the recording medium was sealed under the provisions of Article 25, paragraph (2) and the name of the observer who

sealed the recording medium; and

(xii) beyond what is set forth in the preceding items, the particulars specified by the Rules of the Supreme Court with regard to the circumstances of the implementation of interception under the provisions of Article 20, paragraph (1) or the implementation of reproduction under the provisions of Article 21, paragraph (1).

(2) Notwithstanding the provisions of paragraph (2) of the preceding Article, if the period of conducting the implementation of interception contains a period during which the implementation of interception under the provisions of Article 23, paragraph (1), item (ii) was conducted, a public prosecutor or judicial police officer must submit to the judge prescribed in Article 25, paragraph (4) a document stating the particulars set forth in the items of paragraph (2) of the preceding Article for a period other than the relevant period and the following particulars for the period during which the implementation of interception under the provisions of Article 23, paragraph (1), item (ii) was conducted, respectively, without delay after the termination of the implementation of interception (when there are any encrypted signals temporarily stored under the provisions of that item that have not been decrypted under the provisions of Article 23, paragraph (4) at the time of terminating the implementation of interception, after the termination of the implementation of reproduction). The same applies when a public prosecutor or judicial police officer files a request for the extension of the period during which interception is authorized under the provisions of Article 7 after conducting interception under the provisions of that item:

(i) the date and time of commencement, any suspension, and termination of the implementation of interception under the provisions of Article 23, paragraph (1), item (ii);

(ii) the date and time of commencement and termination of conversations that took place during the implementation of interception under the provisions of Article 23, paragraph (1), item (ii);

(iii) the date and time of commencement, any suspension, and termination of the implementation of reproduction under the provisions of Article 23, paragraph (4);

(iv) particulars sufficient to identify the parts of the conversations prescribed in item (ii) that respectively correspond to encrypted signals that have been decrypted under the provisions of Article 23, paragraph (4), encrypted signals which were deleted before the decryption under the provisions of that paragraph, and any other encrypted signals;

(v) with regard to communications reproduced under the provisions of Article 23, paragraph (4), the provisions that served as the basis for the reproduction, the date and time of commencement and termination of the

reproduced communication, and the names and other particulars that contribute to identification of the parties to the communications;

(vi) with regard to the communications prescribed in Article 15, the name of the offense relating to the communications and the applicable penal statute, as well as the reason for finding that the communications fall under the communications prescribed in that Article;

(vii) the date and time of any replacement of the recording medium during the implementation of reproduction; and

(viii) beyond what is set forth in the preceding items, the particulars specified by the Rules of the Supreme Court with regard to the circumstances of the implementation of interception under the provisions of Article 23, paragraph (1), item (ii) or implementation of reproduction under the provisions of paragraph (4) of that Article.

(3) A judge who has received a document submitted as prescribed in the preceding two paragraphs is to examine whether the communications referred to in paragraph (1), item (vi) or paragraph (2), item (iv) of the preceding Article, or paragraph (1), item (ix), or item (vi) of the preceding paragraph fall under the communications prescribed in Article 15, and when the judge finds that they do not fall under the communications prescribed in Article 15, the judge is to revoke the dispositions for interception or reproduction for the relevant communications. In this case, the provisions of Article 33, paragraphs (3), (5) and (6) apply mutatis mutandis.

(Preparation of an Interception Record)

Article 29 (1) Each time a public prosecutor or judicial police officer has suspended or terminated the implementation of interception (excluding the implementation of interception under the provisions of Article 20, paragraph (1) or Article 23, paragraph (1), item (ii); hereinafter the same applies in this paragraph), the public prosecutor or judicial police officer must promptly prepare a copy of record for the purpose of using the content of the intercepted communications in criminal procedures. The same applies when a recording medium is replaced during the implementation of interception or otherwise recording in a recording medium has been terminated.

(2) Each time a public prosecutor or judicial police officer has suspended or terminated the implementation of reproduction, the public prosecutor or judicial police officer must promptly prepare a copy of record for the purpose of using the content of the reproduced communications in criminal procedures. The same applies when a recording medium is replaced during the implementation of reproduction or otherwise recording in a recording medium has been terminated.

(3) The record prescribed in paragraph (1) is to be prepared by deleting records of

communications other than the following communications from the recording medium in which recording has been made under the provisions of the second sentence of Article 24, paragraph (1) or Article 26, paragraph (2) or a copy of the recording medium set forth in Article 25, paragraph (1) that has been made under the provisions of paragraph (3) of that Article:

(i) communications falling under communications to be intercepted;

(ii) communications intercepted under the provisions of Article 14, paragraph (2) that still require measures for restoring the content thereof;

(iii) communications intercepted under the provisions of Article 15 and communications intercepted under the provisions of Article 14, paragraph (2) that have come to be found to fall under the communications prescribed in Article 15; and

(iv) communications that took place on the same occasion of conversations as the communications set forth in the preceding three items.

(4) The record prescribed in paragraph (2) is to be prepared by deleting records of communications other than the following communications from the recording medium in which recording has been made under the provisions of the second sentence of Article 24, paragraph (1) or Article 26, paragraph (2) or a copy of the recording medium set forth in Article 25, paragraph (2) that has been made under the provisions of paragraph (3) of that Article:

(i) communications falling under communications to be intercepted;

(ii) communications reproduced under the provisions of Article 21, paragraph (4) (including the case in accordance with those provisions in Article 23, paragraph (4); the same applies in the following item) that still require measures for restoring the content thereof;

(iii) communications reproduced under the provisions of Article 21, paragraph (5) (including the case in accordance with those provisions in Article 23, paragraph (4)) and communications reproduced under the provisions of Article 21, paragraph (4) that have come to be found to fall under the communications prescribed in Article 15; and

(iv) communications that took place on the same occasion of conversations as the communications set forth in the preceding three items.

(5) When the communications set forth in paragraph (3), item (ii) or item (ii) of the preceding paragraph are found not to fall under communications to be intercepted and the communications prescribed in Article 15, a record of those communications and a record of the communications set forth in paragraph (3), item (iv) or item (iv) of the preceding paragraph that pertains to those communications must be deleted from the record prescribed in paragraph (1) or the record prescribed in paragraph (2) (hereinafter, collectively referred to as an "interception record"); provided, however, that this does not apply when any of the communications set forth in paragraph (3), items (i) through (iii) or

items (i) through (iii) of the preceding paragraph took place on the same occasion of conversations as those communications.

(6) When a public prosecutor or judicial police officer has prepared an interception record, and when there are any recording media in which intercepted communications (including communications reproduced under the provisions of Article 21, paragraph (1) or Article 23, paragraph (4) and communications restored through decryption under these provisions; the same applies in the following paragraph) are recorded or a copy, etc. (meaning a copy or other article and document recording the whole or part of the content of the record as it is; the same applies hereinafter) thereof, other than the recording medium that the public prosecutor or judicial police officer had submitted to a judge under the provisions of Article 25, paragraph (4) or Article 26, paragraph (4) (hereinafter referred to as the "original record of interception"), all those records must be deleted. The same applies when any records have been deleted from an interception record under the provisions of the preceding paragraph and there still are other copies, etc. of those records.

(7) With regard to intercepted communications other than those recorded in an interception record, a public prosecutor or judicial police officer must not disclose the content thereof to third parties or use the content thereof. The same applies even after a public prosecutor or judicial police officer has left their position.

(Notice to Parties to Communications)

Article 30 (1) A public prosecutor or judicial police officer must give a written notice stating the fact that an interception record has been prepared and the following matters to the parties to the communications recorded in the interception record:

(i) the dates and times of commencement and termination of the communications and the names of the other parties (limited to the case where the names of the other parties are known);

(ii) the date of issuance of the warrant for interception;

(iii) the dates of commencement and termination of the implementation of interception;

(iv) the means of communication subject to the implementation of interception;

(v) the name of the offense and the applicable penal statute stated in the warrant for interception;

(vi) with regard to the communications prescribed in Article 15, to that effect and the name of the offense relating to the communications and the applicable penal statute; and

(vii) the fact that the party may do hearing, etc. (meaning hearing, inspection or copying; hereinafter the same applies in this item) of the interception

record under the provisions of the following Article and a request for permission for hearing, etc. of the original record of interception under the provisions of Article 32, paragraph (1), and an appeal under the provisions of Article 33, paragraph (1) or (2) may be filed.

(2) A notice referred to in the preceding paragraph must be given within 30 days after the termination of the implementation of interception except for the case where the parties to the communications cannot be identified or their whereabouts are not known; provided, however, that when a judge of a district court finds that there is a risk that the investigation will be hindered, the judge may extend the period during which a notice must be given under the provisions of this paragraph by specifying a period not exceeding 60 days upon a request by a public prosecutor or judicial police officer.

(3) In the case where the parties to the communications have been identified or their whereabouts have come to be known after the lapse of the period prescribed in the main clause of the preceding paragraph, a public prosecutor or judicial police officer must promptly give a notice referred to in paragraph (1) to the parties to the communications. In this case, the provisions of the proviso to the preceding paragraph apply mutatis mutandis.

(Hearing and Inspection of an Interception Record)

Article 31 The parties to the communications who have received a notice referred to in paragraph (1) of the preceding Article may hear, inspect or copy the part of the interception record that pertains to the relevant communications.

(Hearing and Inspection of the Original Record of Interception)

Article 32 (1) In the case where a party to the communications recorded in an interception record has heard, inspected or copied the part of the interception record that pertains to the relevant communications as prescribed in the preceding Article, and when a judge who keeps the original record of interception (hereinafter referred to as a "judge keeping the original record") finds it necessary for confirming the accuracy of the interception record or otherwise finds that there are justifiable grounds, the judge must permit hearing, inspection or copying of the part of the original record of interception that corresponds to the relevant communications upon a request by the party to the communications.

(2) When a judge keeping the original record finds it necessary for confirming the content of the intercepted communications (in the case of interception under the provisions of Article 20, paragraph (1) or Article 23, paragraph (1), item (ii), communications reproduced under the provisions of Article 21, paragraph (1) or Article 23, paragraph (4)) or otherwise finds that there are justifiable

grounds, the judge must permit hearing, inspection or copying of the part of the original record of interception that pertains to the relevant communications upon a request by a party to the communications other than the communications recorded in an interception record.

(3) When a judge keeping the original record finds it necessary for proving or disproving of the facts of the crime or confirming the accuracy of an interception record or otherwise finds that there are justifiable grounds with regard to the case for which interception has been conducted, the judge may permit hearing, inspection or copying of the part of the original record of interception that the judge finds necessary upon a request by a public prosecutor or judicial police officer; provided, however, that copying is limited to the part pertaining to the following communications (excluding communications recorded in an interception record):

(i) communications falling under communications to be intercepted;

(ii) communications that serve as evidence necessary to prove or disprove the facts of the crime (excluding the communications set forth in the preceding item); or

(iii) communications that took place on the same occasion of conversations as the communications set forth in the preceding two items.

(4) Notwithstanding the provisions of the preceding paragraph, in the case where there is a judicial decision that ordered deletion of a record pursuant to the provisions of paragraph (3) of the following Article (including the case as applied mutatis mutandis pursuant to Article 27, paragraph (3) and Article 28, paragraph (3); hereinafter the same applies in this paragraph), a request for permission for copying under the provisions of the preceding paragraph may be filed only if those communications pertaining to the record whose deletion was ordered are newly found to fall under the communications set forth in item (i) or (ii) of the preceding paragraph for which there is no other appropriate method of proof to be used in lieu thereof, with regard only to the part of the original record of interception that pertains to the relevant communications and communications that took place on the same occasion of conversations as those communications; provided, however, that this request may not be filed if the judicial decision ordered deletion of the record of these communications on the grounds that the case falls under paragraph (3), item (ii) of the following Article.

(5) With regard to a case under public prosecution for which a request for examination of an interception record or a copy, etc. thereof has been filed by a public prosecutor, when a judge keeping the original record finds it necessary for the defense of the accused or for confirming the accuracy of the interception record, or otherwise finds that there are justifiable grounds, the judge may permit hearing, inspection or copying of the part of the original record of

interception that the judge finds necessary upon a request by the accused or their defense counsel; provided, however, that copying of the part pertaining to the communications to which the accused is not the party is permitted only in the case where there is a consent of one of the parties to the relevant communications.

(6) A copy made by a public prosecutor or judicial police officer under the provisions of paragraph (3) is deemed to be an interception record. In this case, with regard to the application of the provisions of Article 30, the term "and the following matters" in paragraph (1) of that Article is replaced with ", the following particulars, the fact that copying under the provisions of Article 32, paragraph (3) has been permitted, and the date of the permission" and the term "after the termination of the implementation of interception" in paragraph (2) of that Article is replaced with "after making a copy".

(7) Hearing, inspection or copying must not be permitted for the original record of interception except for cases under the provisions of paragraphs (1) through (5); provided, however, that this does not apply in the case where a court or judge, as prescribed in the Code of Criminal Procedure, finds it necessary for proceedings or a judicial decision concerning a case under public prosecution for which a request for examination of an interception record or a copy, etc. thereof has been filed by a public prosecutor or a criminal case relating to interception, and examines the part of the original record of interception that the court or judge finds necessary.

(Appeal)

Article 33 (1) A person who is dissatisfied with a judicial decision rendered by a judge in relation to communications interception may file a request for revocation or modification of the judicial decision with the court to which the judge concerned belongs.

(2) A person who is dissatisfied with dispositions taken by a public prosecutor or public prosecutor's assistant officer in relation to interception or reproduction of communications may file a request for revocation or modification of the dispositions (including the termination of the implementation of interception or the implementation of reproduction; hereinafter the same applies in this paragraph) with the district court having jurisdiction over the location of the public prosecutors office to which the public prosecutor or public prosecutor's assistant officer belongs, and a person who is dissatisfied with dispositions taken by a judicial police official in relation to interception or reproduction of communications may file a request for revocation or modification of the dispositions with the district court having jurisdiction over the place where the official executes their duties.

(3) When a court finds that the case falls under any of the following items upon

revoking measures of interception or reproduction based on a request referred to in the preceding paragraph, the court must order a public prosecutor or judicial police officer to delete: out of the interception record (excluding a record deemed to be an interception record under the provisions of paragraph (6) of the preceding Article; hereinafter the same applies in this paragraph) and a copy, etc. thereof that the public prosecutor or judicial police officer keeps, the record of communications pertaining to the relevant dispositions of interception or reproduction and the record of communications that took place on the same occasion of conversations as those communications, and encrypted signals temporarily stored in relation to the relevant dispositions of interception; provided, however, that this does not apply when a court finds that the case falls under item (iii) and finds it inappropriate to order the deletion of the record:

(i) when the communications pertaining to the relevant interception or reproduction do not fall under any of the communications set forth in the items of paragraph (3) or the items of paragraph (4) of Article 29;

(ii) when there is a serious illegality in procedures for protecting interests of the parties to the communications in conducting interception or reproduction; or

(iii) when there is illegality in procedures for the interception or reproduction except for cases falling under the preceding two items.

(4) When permission for copying referred to in paragraph (3) of the preceding Article has been revoked, a public prosecutor or judicial police officer must delete: out of the record deemed to be an interception record under the provisions of paragraph (6) of that Article (including a copy, etc. thereof) that the public prosecutor or judicial police officer keeps, the part pertaining to the revoked permission.

(5) A judicial decision to order the deletion of a record under the provisions of paragraph (3) or a judicial decision to revoke permission for copying under the provisions of the preceding paragraph does not preclude an interception record or a copy, etc. thereof from being used as evidence in the procedures relating to a case under public prosecution when the examination of evidence has already been conducted for the relevant interception record or a copy, etc. thereof in that case under public prosecution, as long as a decision to exclude from evidence has not been rendered.

(6) When a judicial decision prescribed in the provisions of the preceding paragraph has been rendered for an interception record for which the examination of evidence has already been conducted in a case under public prosecution, the relevant interception record is deemed to have been deleted based on a juridical decision referred to in paragraph (3) or under the provisions of paragraph (4) in applying Article 29, paragraph (7) in cases other

than the case where the content of the interception record is to be made known to third parties or is to be used in the procedures relating to that case under public prosecution.

(7) Beyond what is provided for in this Act, procedures for appeal under the provisions of paragraphs (1) and (2) are to be governed by the procedures for requests referred to in Article 429, paragraph (1) and Article 430, paragraph (1) of the Code of Criminal Procedure.

(Period to Keep the Original Record of Interception)

Article 34 (1) The original record of interception is to be kept until the day on which five years elapse from the day of the submission under the provisions of Article 25, paragraph (4) or Article 26, paragraph (4) or a day on which six months elapse from the day of the conclusion of a case under public prosecution in which an interception record or a copy, etc. thereof was examined as evidence, or the conclusion of a criminal case relating to interception, whichever comes the latest.

(2) When a judge keeping the original record finds it necessary, the judge may extend the period to keep the original record of interception referred to in the preceding paragraph.

Chapter IV Respect of Secrecy of Communications

(Respect of Secrecy of Communications by Persons Concerned)

Article 35 A public prosecutor, public prosecutor's assistant officer, judicial police official, defense counsel, or other person who became involved in interception or reproduction of communications or who has learned the circumstances of interception or reproduction of communications or the content of the intercepted communications (including reproduced communications) in the course of duties must pay attention not to unduly harm the secrecy of communications and not to hinder investigations.

(Report to the Diet)

Article 36 Every year, the national government is to make a report to the Diet on the number of requests for and issuance of warrants for interception, names of offenses pertaining to those requests for and issuance of warrants for interception, types of means of communication subject to interception, period of conducting the implementation of interception, the number of occasions of conversations during the implementation of interception, the number of occasions during which the communications set forth in paragraph (3), item (i) or (iii) or paragraph (4), item (i) or (iii) of Article 29 took place out of those occasions, in cases where the implementation of interception under the

provisions of Article 20, paragraph (1) or Article 23, paragraph (1), item (i) or (ii) was conducted, to that effect, as well as the number of persons who were arrested in relation to cases for which interception was conducted, and also publicize these particulars; provided, however, that when reporting and publication of names of offenses may cause hindrance to investigations, the reporting and publication are to be made after the hindrance ceases to exist.

(Punishment for Acts Violating the Secrecy of Communications)

Article 37 (1) A public employee who has the authority to conduct an investigation or examination to who has committed a crime referred to in Article 179, paragraph (1) of the Telecommunications Business Act (Act No. 86 of 1984) or Article 14, paragraph (1) of the Cable Telecommunications Act (Act No. 96 of 1953) in relation to the duties for the investigation or examination is to be punished by imprisonment for not more than three years or a fine of not more than one million yen.

(2) An attempt of the crime referred to in the preceding paragraph is to be punished.

(3) A person who has filed a complaint or an accusation for any of the crimes referred to in the preceding two paragraphs may file a request referred to in Article 262, paragraph (1) of the Code of Criminal Procedure, if dissatisfied with a disposition by a public prosecutor not to prosecute the relevant crime.

Chapter V Auxiliary Provisions

(Relationship with the Code of Criminal Procedure)

Article 38 Beyond what is specially provided for in this Act, procedures concerning communications interception are to be governed by the Code of Criminal Procedure.

(Rules of the Supreme Court)

Article 39 Beyond what is provided for in this Act, necessary particulars concerning the issuance of a warrant for interception, the extension of the period during which interception is authorized, sealing and submission of a recording medium, storage and other handling of the original record of interception, submission of a document stating the status of the implementation of interception, examination as to whether communications fall under the communications prescribed in Article 15, the extension of the period during which a notice must be given to the parties to the communications, hearing, inspection and copying of an interception record kept by a court, and procedures for filing an appeal are to be provided by Rules of the Supreme Court.

Supplementary Provisions

(Effective Date)

(1) This Act comes into effect as of the day specified by Cabinet Order within a period not exceeding one year from the date of promulgation.
[Effective as of August 15, 2000, under Cabinet Order No. 390 of July 2000]

(Partial Amendment of the Cable Telecommunications Act)

(2) The Cable Telecommunications Act is partially amended as follows:
[The details of the amendment are omitted.]

(Partial Amendment of the Telecommunications Business Act)

(3) The Telecommunications Business Act is partially amended as follows:
[The details of the amendment are omitted.]

Supplementary Provisions [Act No. 160 of December 22, 1999] [Extract]

(Transitional Measures Concerning Dispositions and Applications)

Article 1301 (1) A license, permission, authorization, approval, designation, or other disposition, or a notice or other act that the former organ of the national government has granted or conducted under the provisions of laws and regulations prior to the enforcement of the Acts Related to the Central Government Reform and this Act (hereinafter collectively referred to as the "Reform-related Acts, etc.") is deemed, after the enforcement of the Reform-related Acts, to be a license, permission, authorization, approval, designation, or other disposition, or a notice or other act that the relevant organ of the national government has granted or conducted based on the relevant provisions of laws and regulations after the enforcement of the Reform-related Acts, etc., unless otherwise provided for in laws and regulations.

(2) An application, notification or other act that has been filed or conducted with the former organ of the national government under the provisions of laws and regulations as of the time of the enforcement of the Reform-related Acts, etc. is deemed, after the enforcement of the Reform-related Acts, to be an application, notification or other act that has been filed or conducted with the relevant organ of the national government based on the relevant provisions of laws and regulations after the enforcement of the Reform-related Acts, etc., unless otherwise provided for in laws and regulations.

(3) With regard to the particulars for which reporting, notification, submission or other procedures must be conducted for the former organ of the national government under the provisions of laws and regulations prior to the

enforcement of the Reform-related Acts, etc., and for which such procedures have not been conducted prior to the effective date of the Reform-related Acts, etc., the provisions of laws and regulations after the enforcement of the Reform-related Acts, etc. apply after the enforcement of the Reform-related Acts, etc. by deeming those particulars as the particulars for which reporting, notification, submission or other procedures must be conducted for the relevant organ of the national government under the relevant provisions of laws and regulations after the enforcement of the Reform-related Acts, etc. and for which such procedures have not been conducted, unless otherwise provided for in laws and regulations.

(Transitional Measures Concerning Dispositions Governed by Prior Laws)

Article 1302 With regard to a license, permission, authorization, approval, designation, or other disposition, or a notice or other act that the former organ of the national government is to grant or conduct, or an application, notification or other act that is to be filed or conducted with the former organ of the national government under the laws and regulations providing that prior laws continue to govern, after the enforcement of the Reform-related Acts, etc., the relevant organ of the national government is to grant or conduct such license, permission, authorization, approval, designation, or other disposition, or a notice or other act, and such application, notification or other act is to be filed with the relevant organ of the national government, in accordance with the categories of duties and affairs under jurisdiction of respective organs based on the provisions of laws and regulations after the enforcement of the Reform-related Acts, etc., unless otherwise provided for in laws and regulations.

(Transitional Measures Concerning Penal Provisions)

Article 1303 Prior laws continue to govern the application of penal provisions to acts committed before the enforcement of the Reform-related Acts, etc.

(Delegation to Cabinet Order)

Article 1344 Beyond what is provided for in Articles 71 through 76 and Article 1301 through the preceding Article, and in the Reform-related Acts, etc., Cabinet Order prescribes the necessary transitional measures (including transitional measures concerning penal provisions) concerning the enforcement of the Reform-related Acts, etc.

Supplementary Provisions [Act No. 160 of December 22, 1999] [Extract]

(Effective Date)

Article 1 This Act (excluding Articles 2 and 3) comes into effect as of January 6,

2001; provided, however, that the provisions set forth in the following items come into effect as of the date respectively specified therein:
(i) [Omitted] the provisions of Article 1344: the date of promulgation;
(ii) [Omitted].

Supplementary Provisions [Act No. 153 of December 12, 2001] [Extract]

(Effective Date)
Article 1 (1) This Act comes into effect as of the day specified by Cabinet Order within a period not exceeding six months from the date of promulgation.
[Effective as of March 1, 2002, under Cabinet Order No. 3 of January 2002]

Supplementary Provisions [Act No. 125 of July 24, 2003] [Extract]

(Effective Date)
Article 1 (1) This Act comes into effect as of the day specified by Cabinet Order within a period not exceeding nine months from the date of promulgation; provided, however, that the provisions set forth in the following items come into effect as of the date respectively specified therein:
(i) , (ii) [Omitted];
(iii) [Omitted] the provisions of Article 34 of the Supplementary Provisions to Article 41 of the Supplementary Provisions [Omitted]: the day specified by Cabinet Order within a period not exceeding one year from the date of promulgation.
[Effective as of April 1, 2004, under Cabinet Order No. 58 of March 2004]

Supplementary Provisions [Act No. 120 of November 30, 2007] [Extract]

History

Supplementary Provisions [Act No. 74 of June 24, 2011] [Extract]

(Effective Date)
Article 1 This Act comes into effect as of the day on which twenty days elapse from the date of promulgation. [Omitted]

Supplementary Provisions [Act No. 54 of June 3, 2016] [Extract]

(Effective Date)
Article 1 (1) This Act comes into effect as of the day specified by Cabinet Order within a period not exceeding three years from the date of promulgation;

provided, however, that the provisions set forth in the following items come into effect as of the date respectively specified therein:

[Effective as of June 1, 2019, under Cabinet Order No. 156 of April 2019]

(i) the provisions of Article 9, paragraph (3) of the Supplementary Provisions: the date of promulgation;

(ii) [Omitted]; and

(iii) the provisions of Article 1 (excluding the amending provisions set forth in the preceding item) and Article 6 [Omitted]: the day specified by Cabinet Order within a period not exceeding six months from the date of promulgation;

[Effective as of December 1, 2016, under Cabinet Order No. 316 of September 2016]

(iv) [Omitted].

(Review)

Article 9 (1) In light of the fact that the sound and video recording of interrogations (meaning recording of the accused's statements and the circumstances during the interrogations in a recording medium by a method of sound and video recording and providing it for establishing proof; hereinafter the same applies in this Article) secures appropriate proof for the voluntariness of the suspect's statements and other matters and also contributes to proper implementation of interrogations, the national government is to review the system of sound and video recording of interrogations, upon the lapse of three years after the enforcement of this Act, in consideration of the actual status of sound and video recording of interrogations and the possibility that sound and video recording of interrogations may cause hindrance or any other harmful effects to investigations, and when finding it necessary, take appropriate measures based on the results of the review.

(2) Beyond what is provided for in the preceding paragraph, upon the lapse of three years after the enforcement of this Act, the national government is to review the status of the enforcement of the provisions after amendment by this Act, and when finding it necessary, take appropriate measures based on the results of the review.

(3) After the promulgation of this Act, the national government is to review the disclosure of evidence in trials seeking retrial, measures concerning concealment of the names of the victims in charging instruments, and measures concerning the protection of witnesses, etc. out of criminal proceedings, etc. promptly as needed.

Supplementary Provisions [Act No. 63 of December 4, 2019] [Extract]

(Effective Date)

Article 1 (1) This Act comes into effect as of the day specified by Cabinet Order within a period not exceeding one year from the date of promulgation; provided, however, that the provisions set forth in the following items come into effect as of the date respectively specified therein:

[Effective as of April 1, 2020, under Cabinet Order No. 39 of March 2020]

(i) the provisions of Article 12 and Article 39 of the Supplementary Provisions: the date of promulgation;

(ii) , (iii) [Omitted]

(Transitional Measures Concerning Penal Provisions)

Article 38 Prior laws continue to govern the application of penal provisions to acts committed before the enforcement of this Act and to acts committed after the enforcement of this Act if prior laws continue to govern pursuant to other provisions of this Act.

(Delegation to Cabinet Order)

Article 39 Beyond what is provided for in these Supplement Provisions, Cabinet Order prescribes the necessary transitional measures (including transitional measures concerning penal provisions) concerning the enforcement of this Act.

Appended Table 1 (Related to Articles 3 and 15)

(i) the crime referred to in Article 24 (Cultivation, Import) or Article 24-2 (Possession, Transfer) of the Cannabis Control Act (Act No. 124 of 1948);

(ii) the crime referred to in Article 41 (Import) or Article 41-2 (Possession, Transfer) of the Stimulants Control Act (Act No. 252 of 1951), the crime referred to in Article 41-3, paragraph (1), item (iii) (Import of Stimulants' Raw Materials) or item (iv) (Manufacture of Stimulants' Raw Materials) of the same Act or the crime set forth in paragraph (2) of that Article (Import of Stimulants' Raw Materials for Profit) in relation to these crimes or an attempt of these crimes, the crime referred to in Article 41-4, paragraph (1), item (iii) (Possession of Stimulants' Raw Materials) or item (iv) (Transfer of Stimulants' Raw Materials) of the same Act or the crime set forth in paragraph (2) of that Article (Possession, Transfer of Stimulants' Raw Materials for Profit) in relation to these crimes or an attempt of these crimes;

(iii) the crime referred to in Article 74 (Act of Causing a Group of Stowaways to Illegally Enter Japan), Article 74-2 (Transportation of a Group of Stowaways), or Article 74-4 (Receipt of a Group of Stowaways) of the Immigration Control and Refugee Recognition Act (Cabinet Order No. 319 of

1951);

(iv) the crime referred to in Article 64 (Import of Diacetylmorphine, etc.), Article 64-2 (Transfer, Possession of Diacetylmorphine, etc.), Article 65 (Import of Narcotics Other than Diacetylmorphine, etc.), Article 66 (Transfer, Possession of Narcotics Other than Diacetylmorphine), Article 66-3 (Import of Psychotropics), or Article 66-4 (Transfer of Psychotropics) of the Narcotics and Psychotropics Control Act (Act No. 14 of 1953);

(v) the crime referred to in Article 31 (Unauthorized Manufacture of Firearms), Article 31-2 (Unauthorized Manufacture of Ammunition), or Article 31-3, item (i) (Unauthorized Manufacture of Arms Other than Firearms or Ammunition) of the Ordnance Manufacturing Act (Act No. 145 of 1953);

(vi) the crime referred to in Article 51 (Cultivation of Poppy, Import of Opium) or Article 52 (Transfer, Possession of Opium) of the Opium Control Act (Act No. 71 of 1954);

(vii) the crime referred to in Articles 31 to 31-4 (Firing, Import, Possession, Transfer of Pistols), Articles 31-7 through 31-9 (Import, Possession, Transfer of Pistol Cartridges), Articles 31-11, paragraph (1), item (ii) (Import of Pistol Parts) or paragraph (2) (Attempts), Article 31-16, paragraph (1), item (ii) (Possession of Pistol Parts) or item (iii) (Transfer of Pistol Parts) or paragraph (2) (Attempts) of the Act for Controlling the Possession of Firearms or Swords and Other Weapons (Act No. 6 of 1958);

(viii) the crime referred to in Article 5 (Illegal Import in the Course of Trade) of the Act Concerning Special Provisions for the Narcotics and Psychotropics Control Act and Other Matters for the Prevention of Activities Encouraging Illicit Conduct and Other Activities Involving Controlled Substances through International Cooperation (Act No. 94 of 1991);

(ix) the crime referred to in Article 3 (Organized Homicide) of the Act on the Punishment of Organized Crime and the Control of Criminal Proceeds (Act No. 136 of 1999) in relation to the crime set forth in paragraph (1), item (vii) of that Article or an attempt of the former crime.

Appended Table 2 (Related to Articles 3 and 15)

(i) the crime referred to in Article 1 (Use of Explosives) or Article 2 (Attempted Use) of the Criminal Regulations to Control Explosives (Cabinet Ordinance No. 32 of 1884);

(ii) (a) the crime referred to in Article 108 (Arson of Inhabited Buildings) of the Penal Code (Act No. 45 of 1907) or an attempt thereof;

(b) the crime referred to in Article 199 (Homicide) of the Penal Code or an attempt thereof;

(c) the crime referred to in Article 204 (Injury) or Article 205 (Injury Causing Death) of the Penal Code;

(d) the crime referred to in Article 220 (Unlawful Capture and Confinement) or Article 221 (Unlawful Capture or Confinement Causing Death or Injury) of the Penal Code;

(e) the crime referred to in Articles 224 through 228 (Kidnapping of Minors, Kidnapping for Profit, Kidnapping for Ransom, Kidnapping for Transportation out of a Country, Human Trafficking, Transporting Kidnapped Persons out of a Country, Delivery of Kidnapped Persons, Attempts) of the Penal Code;

(f) the crime referred to in Article 235 (Theft), Article 236, paragraph (1) (Robbery), or Article 240 (Robbery Causing Death or Injury) of the Penal Code or an attempt of these crimes;

(g) the crime referred to in Article 246, paragraph (1) (Fraud), Article 246-2 (Computer Fraud), or Article 249, paragraph (1) (Extortion) of the Penal Code or an attempt of these crimes;

(iii) the crime referred to in Article 7, paragraph (6) (Provision of Child Pornography to Many or Unspecified Persons) or paragraph (7) (Production of Child Pornography for the Provision to Many or Unspecified Persons) of the Act on Punishment of Activities Relating to Child Prostitution and Child Pornography, and the Protection of Children (Act No. 52 of 1999).