Act on Prohibition of Unauthorized Computer Access (Tentative translation)

Act No.128 of 1999
Amendment: Act No.160 of 1999
Amendment: Act No.12 of 2012
Amendment: Act No.28 of 2013

(Purpose)

Article 1 The purpose of this Act is to prevent computer-related crimes committed via telecommunications links and maintain telecommunications-related order as realized by means of access control features by prohibiting acts of unauthorized computer access and stipulating penalties therefor and assistance measures to be taken by prefectural public safety commissions to prevent the recurrence of such acts, thereby contributing to the sound development of an advanced information and telecommunications society.

(Definitions)

Article 2 The term “access administrator” as used in this Act means a person who manages the operation of a computer connected to a telecommunications link (hereinafter referred to as a “specified computer”) in relation to its use (limited to the kind realized via the telecommunications link concerned, hereinafter referred to as “specified use”).

(2) The term “identification code” as used in this Act means a code allocated to a person who, with regard to the specified use of a specified computer, has been granted permission from the access administrator with authority over said specified use (hereinafter referred to as an “authorized user”) or the access administrator himself/herself (hereafter in this paragraph referred to as an “authorized user or the like”) so as to enable the access administrator concerned to identify this particular user or the like as distinguished from all other authorized users and the like. In concrete terms, it may be any of the following or a combination of any of the following and another code:

(i) A code whose content must not, according to the instructions of the access administrator concerned, be revealed to a third party without reason

(ii) A code that has been generated from an image of the whole or a part of the body of the authorized user or the like concerned or his/her voice using a method specified by the access administrator concerned

(iii) A code that has been generated from the signature of the authorized user or the like concerned using a method specified by the access administrator concerned

(3) The term “access control feature” as used in this Act means a feature that has been added to a specified computer subject to specified use or another specified computer connected thereto via a telecommunications link by the access administrator with authority over the specified use of the specified computer concerned to automatically control said specified use. It shall be designed to remove all or part of the restrictions imposed on said specified use upon confirming that a

code input into the specified computer associated therewith by a person wishing to engage in said specified use is identical with the identification code associated with said specified use (including a combination of a code generated from the identification code using a method specified by the access administrator concerned and a part of the identification code concerned, the same applying in items (ⅰ) and (ⅱ) of the following paragraph).

(4) The term “act of unauthorized computer access” as used in this Act means any of the following:

(ⅰ) An act of rendering a specified computer with an access control feature available for specified use that is subject to restrictions imposed by the access control feature concerned by inputting someone else's identification code associated with the access control feature concerned via a telecommunications link and thus operating the specified computer concerned (excluding such an act engaged in by the access administrator who has added the access control feature concerned and upon obtaining permission from the access administrator concerned or the authorized user to whom the identification code concerned belongs)

(ⅱ) An act of rendering a specified computer with an access control feature available for specified use that is subject to restrictions imposed by the access control feature concerned by inputting any information (excluding an identification code) or command suitable for evading the restrictions on said specified use via a telecommunications link and thus operating the specified computer concerned (excluding such an act engaged in by the access administrator who has added the access control feature concerned and upon obtaining permission from the access administrator concerned, the same applying in the following item)

(ⅲ) An act of rendering a specified computer available for specified use that is subject to restrictions imposed by the access control feature of another specified computer connected thereto via a telecommunications link by inputting any information or command suitable for evading said restrictions into this other computer via a telecommunications link and thus operating the specified computer concerned

(Prohibition of acts of unauthorized computer access)

Article 3 No person shall engage in an act of unauthorized computer access.

(Prohibition of acts of obtaining someone else's identification code)

Article 4 No person shall obtain someone else's identification code associated with an access control feature to engage in an act of unauthorized computer access (limited to the kind specified in Article 2, paragraph (4) item (ⅰ), the same applying in Article 6 and Article 12, item (ⅱ)).

(Prohibition of acts of facilitating unauthorized computer access)

Article 5 No person shall, unless there are justifiable grounds for refusing to do so or any other legitimate reason therefor, supply someone else's identification code associated with an access control feature to a person other than the access administrator associated with the access control feature concerned and the authorized user to whom the identification code concerned belongs.

(Prohibition of acts of wrongful storing someone else's identification code)

Article 6 No person shall store someone else's identification code associated with an access control feature that has been wrongfully obtained to engage in an act of unauthorized computer access.

(Prohibition of acts of illicitly requesting input of identification code)

Article 7 No person shall engage in any of the acts listed below by impersonating an access administrator who has added an access control feature to a specified computer or otherwise creating a false impression of him/her being the access administrator concerned. However, this shall not apply if permission has been obtained from the access administrator concerned.

(ⅰ) An act of leaving the following false information accessible to the general public via automatic public transmission carried out through connection to a telecommunications link (the kind designed for on-demand activation and direct reception by the general public, excluding broadcasting or cable broadcasting): information purporting to be the access administrator concerned requesting an authorized user who has been allocated an identification code associated with the access control feature concerned to input the identification code concerned into a specified computer

(ⅱ) An act of transmitting the following false information to the authorized user concerned via an email (an email as specified in Article 2, item (ⅰ), of the Act on Regulation of Transmission of Specified Electric Mail (Act No. 26 of 2002): information purporting to be the access administrator concerned requesting an authorized user who has been allocated an identification code associated with the access control feature concerned to input the identification code concerned into a specified computer

(Protective measures by access administrators)

Article 8 An access administrator who has added an access control feature to a specified computer shall endeavor to properly manage identification codes associated with the access control feature concerned or codes used to confirm them via the access control feature concerned, and shall always verify the effectiveness of the access control feature concerned, with efforts made to promptly take appropriate measures to protect the specified computer concerned from acts of unauthorized computer access, such as an enhancement of the function of the access control feature concerned, whenever deemed necessary.

(Assistance, etc. by prefectural public safety commissions)

Article 9 A prefectural public safety commission (a Area public safety commission in the case of areas (as specified in the main clause of Article 51, paragraph (1), of the Police Act (Act No.162 of 1954), the same applying hereafter in this paragraph) other than the one containing the seat of the Hokkaido Prefectural Police Headquarters, the same applying hereafter in this article) shall, in the event of recognizing the occurrence of an act of unauthorized computer access, provide the access administrator associated with the specified computer that has been exposed to unauthorized access with appropriate assistance, including advice, guidance and supply of relevant data, so as to enable him/her to take any emergency necessary measures to protect the specified computer concerned from further acts of unauthorized access according to the modus operandi or cause of the act of unauthorized access concerned. This shall be on condition that the access administrator concerned has requested assistance by submitting any documents and other materials useful in ascertaining the operational and management status of the specified computer concerned at the time of the act of unauthorized access concerned and other circumstances to prevent the recurrence of similar acts, and that such a request is deemed reasonable.

(2) A prefectural public safety commission may entrust the whole or a part of the work involved in the implementation of the case analysis needed to provide the assistance prescribed in the preceding paragraph (encompassing a technical investigation and analysis of the modus operandi and cause of the act of unauthorized computer access for which the assistance concerned has been sought and other matters, the same applying in the following paragraph) to a person to be specified in the Rules of National Public Safety Commission.

(3) Any person who has engaged in the work involved in the implementation of the case analysis entrusted by a prefectural public safety commission pursuant to the provision of the preceding paragraph shall not divulge any secrets he/she has become privy to through this work.

(4) Any necessary matters in connection with the assistance prescribed in paragraph (1), in addition to what is provided for in the preceding three paragraphs, shall be prescribed by the Rules of Nationa1 Public Safety Commission.

(5) A prefectural public safety commission shall, in addition to what is provided for in paragraph (1), endeavor to raise awareness and spread knowledge about the protection of specified computers with an access control feature from acts of unauthorized computer access.

Article 10 The National Public Safety Commission, Minister for Internal Affairs and Telecommunications, and Minister of Economy, Trade and Industry shall, to help protect specified computers with an access control feature from acts of unauthorized computer access, publicize the status of the occurrence of acts of unauthorized computer access and progress of research and development on technology relating to access control features at least once a year.

(2) The National Public Safety Commission, Minister for Internal Affairs and Telecommunications, and Minister of Economy, Trade and Industry must, to help protect specified computers with an access control feature from acts of unauthorized computer access, endeavor to assist any organizations formed by persons who engage in business activities geared towards the enhancement of access control features for the purpose of assisting in measures taken by access administrators who have added access control features to specified computers pursuant to the provisions of Article 8 through the supply of the necessary information and so on, provided that they are deemed to be capable of providing such assistance appropriately and effectively.

(3) In addition to what is provided for in the preceding two paragraphs, the National Government shall endeavor to raise awareness and spread knowledge about the protection of specified computers with an access control feature from acts of unauthorized computer access.

(Penal provisions)

Article 11 Any person who has violated the provisions of Article 3 shall be punished by imprisonment with work for not more than three years or a fine of not more than 1 million yen.

Article 12 Any person who falls under any of the following items shall be punished by imprisonment with work for not more than one year or a fine of not more than 500,000 yen.

(i) A person who has violated the provisions of Article 4

(ii) A person who has supplied the identification code of another person in violation of the provisions of Article 5 despite knowing that the recipient intends to use it for an act of unauthorized computer access

(iii) A person who has violated the provisions of Article 6

(iv) A person who has violated the provisions of Article 7

(v) A person who has violated the provisions of paragraph (3) of Article 9

Article 13 Any person who has violated the provisions of Article 5 (excluding a person specified in item (ii) of the preceding article) shall be punished by a fine of not more than 300,000 yen.

Article 14 The offenses specified in Article 11 and Article 12, items (i) to (iii), shall be governed by the provisions of Article 4-2, of the Penal Code (Act No.45 of 1907).

This is unofficial translation. Only the original Japanese text of the law has legal effect, and the translation is to be used solely as reference material to aid in the understanding of Japanese law.

This "Tentative translation" data has not yet been proofread or corrected by a native English speaker or legal translation expert; this data may be revised in the future.