Act on Prohibition of Unauthorized Computer Access

(Act No. 128 of August 13, 1999)

(Purpose)

Article 1 The purpose of this Act is to prevent computer-related crimes committed via telecommunications lines 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 (1) The term "access administrator" as used in this Act means a person who manages the operation of a computer connected to a telecommunications line (hereinafter referred to as a "specified computer") in relation to its use (limited to the kind realized via the telecommunications line 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 the relevant specified use (hereinafter referred to as an "authorized user") or the relevant access administrator (hereafter in this paragraph referred to as an "authorized user, etc.") so as to enable the access administrator concerned to identify this particular authorized user, etc. as distinguished from all other authorized users, etc. In concrete terms, an identification code may be any of the following or a combination of any of the following and another code:

(i) a code the content of which 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, etc. concerned or the relevant user's voice using a method specified by the access administrator concerned

(iii) a code that has been generated from the signature of the authorized user, etc. 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 line by the access administrator with authority over the specified use of the specified computer

concerned to automatically control the relevant specified use. An access control feature is to be designed to remove all or part of the restrictions imposed on the relevant specified use upon confirming that a code input into the specified computer associated therewith by a person wishing to engage in the relevant specified use is identical to the identification code associated with the relevant 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 applies 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 acts:

(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 line and thus operating the specified computer concerned (excluding the relevant act engaged in by the access administrator who has added the access control feature concerned and the relevant act engaged in upon obtaining approval 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 inputting a directive to command suitable for evading the restrictions on the relevant specified use via a telecommunications line and thus operating the specified computer concerned (excluding the relevant act engaged in by the access administrator who has added the access control feature concerned and the relevant act engaged in upon obtaining approval from the access administrator concerned; the same applies 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 line by inputting any information or inputting a directive to command suitable for evading said restrictions into the relevant other specified computer via a telecommunications line and thus operating the specified computer concerned

(Prohibition of Acts of Unauthorized Computer Access)

Article 3 It is prohibited for any person to engage in an act of unauthorized computer access.

(Prohibition of Acts of Obtaining Someone Else's Identification Code)

Article 4 It is prohibited for any person to obtain someone else's identification code associated with an access control feature for the purpose of engaging in an act of unauthorized computer access (limited to the kind specified in Article 2, paragraph (4), item (i); the same applies in Article 6 and Article 12, item (ii)).

(Prohibition of Acts of Facilitating Unauthorized Computer Access)

Article 5 It is prohibited for any person, unless there are legitimate grounds for refusing to do so or any other legitimate reason therefor, to 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 Wrongfully Storing Someone Else's Identification Code)

Article 6 It is prohibited for any person to store someone else's identification code associated with an access control feature that has been wrongfully obtained for the purpose of engaging in an act of unauthorized computer access.

(Prohibition of Acts of Illicitly Requesting the Input of Identification Codes)

Article 7 It is prohibited for any person to 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 being the access administrator concerned; provided however, this does not apply if permission has been obtained from the access administrator concerned.

(i) An act of leaving the following information available for inspection to the general public via automatic public transmission carried out through connection to a telecommunications line (meaning 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 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 Electronic Mail (Act No. 26 of 2002)): information purporting to be from 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 an Access Administrator)

Article 8 An access administrator who has added an access control feature to a specified computer is to 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 is to always inspect the effectiveness of the access control feature concerned and endeavor to promptly take necessary measures to protect the specified computer concerned from acts of unauthorized computer access, such as enhancement of the function of the access control feature concerned, whenever deemed necessary.

(Assistance by Prefectural Public Safety Commissions)

Article 9 (1) In the event of recognizing the occurrence of an act of unauthorized computer access, the prefectural public safety commission (area public safety commission in case of the areas except for the area where Hokkaido Police Headquarters is located (meaning the area prescribed in the main clause of Article 51, paragraph (1) of the Police Act (Act No.162 of 1954); the same applies in this paragraph;); hereinafter the same applies in this Article) is to 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 the relevant administrator to take any necessary emergency 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 is on the condition that the access administrator concerned has requested assistance together with any documents and other items regarding the matters which would serve as reference information such as 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 the relevant 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 applies 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 provisions of the preceding paragraph may not divulge any secrets that said person has become privy to through this work.

(4) Beyond what is set forth in the preceding three paragraphs, any necessary matters in connection with the assistance prescribed in paragraph (1) are prescribed by the Rules of Nationa1 Public Safety Commission.

(5) Beyond what is set forth in paragraph (1), the prefectural public safety commission must 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 (1) To help protect specified computers with an access control feature from acts of unauthorized computer access, the National Public Safety Commission, Minister for Internal Affairs and Telecommunications, and Minister of Economy, Trade and Industry are to 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) To help protect specified computers with an access control feature from acts of unauthorized computer access, the National Public Safety Commission, Minister for Internal Affairs and Telecommunications, and Minister of Economy, Trade and Industry must 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 the relevant assistance appropriately and effectively.

(3) Beyond what is set forth in the preceding two paragraphs, the National Government must 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 is 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 is 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 knowingly 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) is 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), are governed by the provisions of Article 4-2, of the Penal Code (Act No.45 of 1907).