

Unauthorized Computer Access Law (Law No. 128 of 1999)

(provisional translation)

(Purpose)

Article 1. The purpose of this Law is, by prohibiting acts of unauthorized computer access as well as by stipulating penal provisions for such acts and assistance measures to be taken by the Metropolitan or Prefectural Public Safety Commissions for preventing a recurrence of such acts, to prevent computer-related crimes that are committed through telecommunication lines and to maintain the telecommunications-related order that is realized by access control functions, and, thereby, to contribute to the sound development of the advanced information and telecommunications society.

(Definitions)

Article 2. In this law, “access administrator” means a person who administers the operations of a computer (hereafter referred to as “specific computer”) which is connected to a telecommunication line, with regard to its use (limited to such use as is conducted through the telecommunication line concerned; hereafter referred to as “specific use”).

2. In this Law, “identification code” means a code — that is granted to a person (hereafter referred to as “authorized user”) who has been authorized by the access administrator governing a specific use of a specific computer to conduct that specific use, or to that access administrator (hereafter in this paragraph, authorized user and access administrator being referred to as “authorized user, etc.”) to enable that access administrator to identify that authorized user, etc., distinguishing the latter from another authorized user, etc.; and that falls under any of the following items or that is a combination of a code which falls under any of the following items and any other code:

- (1) A code the content of which the access administrator concerned is required not to make known to a third party wantonly;
- (2) A code that is compiled in such ways as are defined by the access administrator concerned using an image of the body, in whole or in part, of the authorized user, etc., concerned, or his or her voice;
- (3) A code that is compiled in such ways as are defined by the access administrator concerned using the signature of the authorized user, etc., concerned.

3. In this Law, “access control function” means a function that is added, by the access administrator governing a specific use, to a specific computer or to another specific computer which is connected to that specific computer through a telecommunication line in order to automatically control the specific use concerned of that specific computer, and that removes all or part of restrictions on that specific use after confirming that a code inputted into a specific computer having that function by a person who is going to conduct that specific use is the identification code (to include a code which is a combination of a code compiled in such ways as are defined by the access administrator concerned using an identification code and part of that identification code; the same shall apply in Article 3, paragraph 2, items (1) and (2)) for that specific use.

(Prohibition of acts of unauthorized computer access)

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

2. The act of unauthorized computer access mentioned in the preceding paragraph means an act that falls under one of the following items:

(1) An act of making available a specific use which is restricted by an access control function by making in operation a specific computer having that access control function through inputting into that specific computer, via telecommunication line, another person’s identification code for that access control function (to exclude such acts conducted by the access administrator who has added the access control function concerned, or conducted with the approval of the access administrator concerned or of the authorized user for that identification code);

(2) An act of making available a restricted specific use by making in operation a specific computer having that access control function through inputting into it, via telecommunication line, any information (excluding an identification code) or command that can evade the restrictions placed by that access control function on that specific use (to exclude such acts conducted by the access administrator who has added the access control function concerned, or conducted with the approval of the access administrator concerned; the same shall apply in the following item);

(3) An act of making available a restricted specific use by making in operation a specific computer, whose specific use is restricted by an access control function installed into another specific computer which is connected, via a telecommunication line, to that specific computer, through inputting into it, via a telecommunication line, any information or command that can evade the restrictions concerned.

(Prohibition of acts of facilitating unauthorized computer access)

Article 4. No person shall provide another person's identification code relating to an access control function to a person other than the access administrator for that access control function or the authorized user for that identification code, in indicating that it is the identification code for which specific computer's specific use, or at the request of a person who has such knowledge, excepting the case where such acts are conducted by that access administrator, or with the approval of that access administrator or of that authorized user.

(Protective measures by access administrators)

Article 5. The access administrator who has added an access control function to a specific computer shall endeavor to properly manage identification codes relating to that access control function and codes used to confirm such identification codes through that access control function, and shall always verify the effectiveness of that access control function, and, when he deems it necessary, shall endeavor to promptly take necessary measures to protect that specific computer from acts of unauthorized computer access, including the upgrading of the access control function concerned.

(Assistance, etc., by Metropolitan and Prefectural Public Safety Commissions)

Article 6. The Metropolitan or Prefectural Public Safety Commission (each of the Area Public Safety Commissions in case of the Areas (that means the Areas mentioned in Article 51, paragraph 1, main part, of the Police Law (Law No. 162 of 1954); the same shall apply hereafter in this paragraph) except the Area which comprises the place of the Hokkaido Prefectural Police Headquarters: the same shall apply hereafter in this Article), in case an act of unauthorized computer access is recognized to have been conducted and if, for the purpose of preventing a recurrence of similar acts, assistance is requested by the access administrator of the specific computer involved in that act of unauthorized computer access, attaching to such request any documents or articles regarding referential matters, such as the situations of operation and management of that specific computer at the time of that act of unauthorized access, shall provide, when it deems such request reasonable, that access administrator with assistance, including provision of relevant materials, advice and guidance, so that necessary emergency measures can be properly taken in

accordance with the modus operandi of that act of unauthorized access or its cause to protect that specific computer from acts of unauthorized access.

2. The Metropolitan or Prefectural Public Safety Commission may entrust to a person to be stipulated by National Public Safety Commission Regulation with all or part of the work of implementing a case analysis (which means making a technical study and analysis on the modus operandi of the act of unauthorized computer access relating to that request and the cause of such act; the same shall apply in the following paragraph) which is necessary for the providing of the assistance mentioned in the preceding paragraph.

3. A person who has engaged in the work of implementing a case analysis entrusted by the Metropolitan or Prefectural Public Safety Commission in accordance with the preceding paragraph shall not reveal secret he or she has learned with regard to such implementation.

4. The necessary matters, other than those stipulated in the preceding three paragraphs, relating to the assistance mentioned in the first paragraph shall be stipulated by National Public Safety Commission Regulation.

Article 7. The National Public Safety Commission, the Minister of International Trade and Industry and the Minister of Posts and Telecommunications shall publicize, at least once a year, the situation of occurrence of acts of unauthorized computer access as well as the situation of research and development of the access control function-related technology in order to help protect specific computers having access control functions from acts of unauthorized computer access.

2. In addition to the preceding paragraph, the State shall endeavor to assure the enlightenment and diffusion of knowledge regarding the protection of specific computers having access control functions from acts of unauthorized computer access.

(Penal provisions)

Article 8. A person who falls under one of the following items shall be punished with penal servitude for not more than one year or a fine of not more than 500,000 yen:

- (1) A person who has infringed the provision of Article 3, paragraph 1;
- (2) A person who has infringed the provision of Article 6, paragraph 3.

Article 9. A person who has infringed the provision of Article 4 shall be punished with a fine of not more than 300,000 yen.

SUPPLEMENTARY PROVISION

This Law shall come into force when the period of six months will have elapsed counting from the date of its promulgation; provided that the provisions of Article 6 and of Article 8, item (2) shall come into force on the date to be stipulated by Cabinet Order within the scope not exceeding one year counting from the date of its promulgation.