不正アクセス行為の禁止等に関する法律
Act on Prohibition of Unauthorized Computer Access

（平成十一年八月十三日法律第百二十八号）
(Act No. 128 of August 13, 1999)

（目的）
(Purpose)

第一条　この法律は、不正アクセス行為を禁止するとともに、これについての罰則及びその再発防止のための都道府県公安委員会による援助措置等を定めることにより、電気通信回線を通じて行われる電子計算機に係る犯罪の防止及びアクセス制御機能により実現される電気通信に関する秩序の維持を図り、もって高度情報通信社会の健全な発展に寄与することを目的とする。

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.

（定義）
(Definitions)

第二条　この法律において「アクセス管理者」とは、電気通信回線に接続している電子計算機（以下「特定電子計算機」という。）の利用（当該電気通信回線を通じて行うものに限る。以下「特定利用」という。）につき当該特定電子計算機の動作を管理する者をいう。

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　この法律において「識別符号」とは、特定電子計算機の特定利用をすることについて当該特定利用に係るアクセス管理者の許諾を得た者（以下「利用権者」という。）及び当該アクセス管理者（以下この項において「利用権者等」という。）に、当該アクセス管理者において当該利用権者等を他の利用権者等と区別して識別することができるように付される符号であって、次のいずれかに該当するもの又は次のいずれかに該当する符号とその他の符号を組み合わせたものをいう。

(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:

一　当該アクセス管理者によってその内容をみだりに第三者に知らせてはならないものとされている符号

(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

二　当該利用権者等の身体の全部若しくは一部の影像又は音声を用いて当該アクセス管理者が定める方法により作成される符号

(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

三　当該利用権者等の署名を用いて当該アクセス管理者が定める方法により作成される符号

(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　この法律において「アクセス制御機能」とは、特定電子計算機の特定利用を自動的に制御するために当該特定利用に係るアクセス管理者によって当該特定電子計算機又は当該特定電子計算機に電気通信回線を介して接続された他の特定電子計算機に付加されている機能であって、当該特定利用をしようとする者により当該機能を有する特定電子計算機に入力された符号が当該特定利用に係る識別符号（識別符号を用いて当該アクセス管理者の定める方法により作成される符号と当該識別符号の一部を組み合わせた符号を含む。次項第一号及び第二号において同じ。）であることを確認して、当該特定利用の制限の全部又は一部を解除するものをいう。

(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　この法律において「不正アクセス行為」とは、次の各号のいずれかに該当する行為をいう。

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

一　アクセス制御機能を有する特定電子計算機に電気通信回線を通じて当該アクセス制御機能に係る他人の識別符号を入力して当該特定電子計算機を作動させ、当該アクセス制御機能により制限されている特定利用をし得る状態にさせる行為（当該アクセス制御機能を付加したアクセス管理者がするもの及び当該アクセス管理者又は当該識別符号に係る利用権者の承諾を得てするものを除く。）

(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)

二　アクセス制御機能を有する特定電子計算機に電気通信回線を通じて当該アクセス制御機能による特定利用の制限を免れることができる情報（識別符号であるものを除く。）又は指令を入力して当該特定電子計算機を作動させ、その制限されている特定利用をし得る状態にさせる行為（当該アクセス制御機能を付加したアクセス管理者がするもの及び当該アクセス管理者の承諾を得てするものを除く。次号において同じ。）

(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)

三　電気通信回線を介して接続された他の特定電子計算機が有するアクセス制御機能によりその特定利用を制限されている特定電子計算機に電気通信回線を通じてその制限を免れることができる情報又は指令を入力して当該特定電子計算機を作動させ、その制限されている特定利用をし得る状態にさせる行為

(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

（不正アクセス行為の禁止）
(Prohibition of Acts of Unauthorized Computer Access)

第三条　何人も、不正アクセス行為をしてはならない。

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

（他人の識別符号を不正に取得する行為の禁止）
(Prohibition of Acts of Obtaining Someone Else's Identification Code)

第四条　何人も、不正アクセス行為（第二条第四項第一号に該当するものに限る。第六条及び第十二条第二号において同じ。）の用に供する目的で、アクセス制御機能に係る他人の識別符号を取得してはならない。

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)).

（不正アクセス行為を助長する行為の禁止）
(Prohibition of Acts of Facilitating Unauthorized Computer Access)

第五条　何人も、業務その他正当な理由による場合を除いては、アクセス制御機能に係る他人の識別符号を、当該アクセス制御機能に係るアクセス管理者及び当該識別符号に係る利用権者以外の者に提供してはならない。

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.

（他人の識別符号を不正に保管する行為の禁止）
(Prohibition of Acts of Wrongfully Storing Someone Else's Identification Code)

第六条　何人も、不正アクセス行為の用に供する目的で、不正に取得されたアクセス制御機能に係る他人の識別符号を保管してはならない。

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.

（識別符号の入力を不正に要求する行為の禁止）

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

第七条　何人も、アクセス制御機能を特定電子計算機に付加したアクセス管理者になりすまし、その他当該アクセス管理者であると誤認させて、次に掲げる行為をしてはならない。ただし、当該アクセス管理者の承諾を得てする場合は、この限りでない。

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.

一　当該アクセス管理者が当該アクセス制御機能に係る識別符号を付された利用権者に対し当該識別符号を特定電子計算機に入力することを求める旨の情報を、電気通信回線に接続して行う自動公衆送信（公衆によって直接受信されることを目的として公衆からの求めに応じ自動的に送信を行うことをいい、放送又は有線放送に該当するものを除く。）を利用して公衆が閲覧することができる状態に置く行為

(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

二　当該アクセス管理者が当該アクセス制御機能に係る識別符号を付された利用権者に対し当該識別符号を特定電子計算機に入力することを求める旨の情報を、電子メール（特定電子メールの送信の適正化等に関する法律（平成十四年法律第二十六号）第二条第一号に規定する電子メールをいう。）により当該利用権者に送信する行為

(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

（アクセス管理者による防御措置）

(Protective Measures by an Access Administrator)

第八条　アクセス制御機能を特定電子計算機に付加したアクセス管理者は、当該アクセ

ス制御機能に係る識別符号又はこれを当該アクセス制御機能により確認するために用いる符号の適正な管理に努めるとともに、常に当該アクセス制御機能の有効性を検証し、必要があると認めるときは速やかにその機能の高度化その他当該特定電子計算機を不正アクセス行為から防御するため必要な措置を講ずるよう努めるものとする。

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.

（都道府県公安委員会による援助等）

(Assistance by Prefectural Public Safety Commissions)

第九条　都道府県公安委員会（道警察本部の所在地を包括する方面（警察法（昭和二十九年法律第百六十二号）第五十一条第一項本文に規定する方面をいう。以下この項において同じ。）を除く方面にあっては、方面公安委員会。以下この条において同じ。）は、不正アクセス行為が行われたと認められる場合において、当該不正アクセス行為に係る特定電子計算機に係るアクセス管理者から、その再発を防止するため、当該不正アクセス行為が行われた際の当該特定電子計算機の作動状況及び管理状況その他の参考となるべき事項に関する書類その他の物件を添えて、援助を受けたい旨の申出があり、その申出を相当と認めるときは、当該アクセス管理者に対し、当該不正アクセス行為の手口又はこれが行われた原因に応じ当該特定電子計算機を不正アクセス行為から防御するため必要な応急の措置が的確に講じられるよう、必要な資料の提供、助言、指導その他の援助を行うものとする。

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　都道府県公安委員会は、前項の規定による援助を行うため必要な事例分析（当該援助に係る不正アクセス行為の手口、それが行われた原因等に関する技術的な調査及び分析を行うことをいう。次項において同じ。）の実施の事務の全部又は一部を国家公安委員会規則で定める者に委託することができる。

(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　前項の規定により都道府県公安委員会が委託した事例分析の実施の事務に従事した者は、その実施に関して知り得た秘密を漏らしてはならない。

(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　前三項に定めるもののほか、第一項の規定による援助に関し必要な事項は、国家公安委員会規則で定める。

(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　第一項に定めるもののほか、都道府県公安委員会は、アクセス制御機能を有する特定電子計算機の不正アクセス行為からの防御に関する啓発及び知識の普及に努めなければならない。

(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.

第十条　国家公安委員会、総務大臣及び経済産業大臣は、アクセス制御機能を有する特定電子計算機の不正アクセス行為からの防御に資するため、毎年少なくとも一回、不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況を公表するものとする。

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　国家公安委員会、総務大臣及び経済産業大臣は、アクセス制御機能を有する特定電子計算機の不正アクセス行為からの防御に資するため、アクセス制御機能を特定電子計算機に付加したアクセス管理者が第八条の規定により講ずる措置を支援することを目的としてアクセス制御機能の高度化に係る事業を行う者が組織する団体であって、当該支援を適正かつ効果的に行うことができると認められるものに対し、必要な情報の提供その他の援助を行うよう努めなければならない。

(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　前二項に定めるもののほか、国は、アクセス制御機能を有する特定電子計算機の不正アクセス行為からの防御に関する啓発及び知識の普及に努めなければならない。

(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.

（罰則）

(Penal provisions)

第十一条　第三条の規定に違反した者は、三年以下の懲役又は百万円以下の罰金に処する。

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.

第十二条　次の各号のいずれかに該当する者は、一年以下の懲役又は五十万円以下の罰金に処する。

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.

一　第四条の規定に違反した者

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

二　第五条の規定に違反して、相手方に不正アクセス行為の用に供する目的があることの情を知ってアクセス制御機能に係る他人の識別符号を提供した者

(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

三　第六条の規定に違反した者

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

四　第七条の規定に違反した者

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

五　第九条第三項の規定に違反した者

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

第十三条　第五条の規定に違反した者（前条第二号に該当する者を除く。）は、三十万円以下の罰金に処する。

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.

第十四条　第十一条及び第十二条第一号から第三号までの罪は、刑法（明治四十年法律第四十五号）第四条の二の例に従う。

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).