PROGRAM ON U.S.-JAPAN RELATIONS
Weatherhead Center FOR INTERNATIONAL AFFAIRS
HARVARD UNIVERSITY

HARVARD
UNIVERSITY

LEGAL FRAMEWORK OF CYBERCRIME INVESTIGATION: THE CURRENT MEANING OF THE CFAA AND COMPARISON TO THE ACT ON PROHIBITION OF UNAUTHORIZED COMPUTER ACCESS

Kei Kitanohara

Harvard Program on U.S.-Japan Relations
Occasional Paper Series
2023-KK

https://programs.wcfia.harvard.edu/us-japan/research

TABLE OF CONTENTS

TABLES AND FIGURES

LIST OF ABBREVIATIONS

APUCA	Act on Prohibition of Unauthorized Computer Access (Act No. 128 of 1999)
CACFAA	Counterfeit Access device and Computer Fraud and Abuse Act of 1984
CFAA	Computer Fraud and Abuse Act of 1986
DDoS	Denial of service
DOJ	Department of Justice
FBI	Federal Bureau of Investigation
IoT	Internet of Things
NPA	National Police Agency of Japan

Introduction

The Increasing Threat of Cybercrimes

"Cybercrimes" are a major issue in today's interconnected world. With an internet connection, people can do almost everything necessary for their lives. Indeed, one might not be able to live without the internet. There are always pros and cons, however, as with the invention of the automobile, which made it easier to move over long distances, but gave rise to the danger of traffic accidents. Cybercrimes have grown exponentially since the term was first introduced, and they are now a worse problem than ever. In the United States, there were 847,376 complaints involving cybercrimes in 2021,[1] and in Japan, there were 12,209 cleared cases during the same year.[2] Thus, it is clear how large the issue of cybercrimes is. The number of cases is just one perspective on the difficulty of cybercrime investigations, but technical issues and jurisdictional problems remain.[3]

Definition of "Cybercrimes"

The term "cybercrimes" has no concrete definition, and this sometimes makes it difficult to discuss the issue. Traditionally, the term "computer crime" or a "computer-related crime" is often used by academic scholars and law enforcement officials in considering today's so-called

---

[1] Internet Crime Complaint Center. *Internet Crime Report 2021*. FBI, Mar. 2022, www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf; In 2022, complaints decreased by 5 percent, 800,944 reported, but it is still a serious problem.

[2] *令和３年におけるサイバー空間をめぐる脅威の情勢等について(Threats Related to Cyber Space in 2021)*. NPA, Apr. 2022, www.npa.go.jp/publications/statistics/cybersecurity/data/R03_cyber_jousei.pdf; The NPA does not release the number of cybercrime cases recognized by police, but it is easy to imagine how many cases there are.

[3] In the United States, the first issue involving cybercrime was its criminal jurisdiction. Since cybercrimes were often conducted across state lines, it was a big problem for law enforcement agencies to determine which laws should be applied and which authorities should investigate the case.

"cybercrimes," and cybercrime is a specific area of computer crime. In this paper, however, I will use cybercrime rather than computer crime because it appears more often and the difference between computer crime and cybercrime has become increasingly vague. At this point, one question may arise: "What, exactly, is cybercrime?" This question differs from scholar to scholar, but there are two or three categories in general. I will choose the categorization that separates "computer misuse crimes" from "traditional crimes."[4] The former is a new type of criminal offense compared to the latter. It is typical that these offensive acts target computers or computer networks and cause malfunctions. Although it has been said that the first cybercrime was uncovered in France in 1836,[5] the United States Comprehensive Crime Prevention Act, the first U.S. federal law that made computer misuse illegal, was enacted in 1984. On the other hand, the "traditional crimes" of cybercrimes are those facilitated by computers or computer networks. These crimes usually are prohibited by the traditional penal code, but are distinguished from traditional crimes by using computers as an essential part of the crime, such as internet fraud schemes, distributing child pornography, stealing secrets, or dealing in drugs over the internet. For the record, the definition of cybercrime given by the Department of Justice is "crimes that use or target computer networks."[6] On the other hand, according to the NPA, a cybercrime is an "incident in which the life, body, and property of an individual, as well as public safety and order, are or may be endangered due to compromised cybersecurity or other illicit activities using

---

[4] Orin S. Kerr, *Computer Crime Law*. Fourth Edition (St. Paul, MN: West Academic Publishing, 2018) 1
[5] Tom Standage, *The Crooked Timber of Humanity*. The Economist, 5 Oct. 2017, Available: www.economist.com/1843/2017/10/05/the-crooked-timber-of-humanity.
[6] H. Marshall Jarrett, et al. *Prosecuting Computer Crimes*. Office of Legal Education Executive Office for United States Attorneys, 2010: v, www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf.

information technology."[7] These government definitions are overly broad and represent how cybercrimes have become so prolific in our society.

Scope of this paper

In this paper, I would like to review the most important cybercrime-related law in the United States, the Computer Fraud and Abuse Act of 1986 (CFAA), compare it to the Japanese legal framework, and consider the future course of cybercrime laws. As I mentioned above, issues related to cybercrimes, such as the technical aspect of conducting cybercrimes, are still one of the biggest problems we face. In terms of the number of cybercrime cases as well, there is a huge difference between the United States and Japan, and many readers might be interested in the reason. I will focus more on legal problems to answer my questions because there are a lot of and a wide variety of possible causes of that, such as victim's awareness, the difference in the internet structure within the country and protocols for reporting to law enforcement, and it is also difficult to discuss them in great detail. Indeed, there is also the issue of jurisdiction because cybercrimes are often conducted in foreign countries, but both law enforcement officers in the United States and Japan are allowed to investigate the cases whose results occur within their territory, so the problem of jurisdiction should not be a big issue at least in terms of investigation. Since the CFAA was enacted about 40 years ago, there have been many court decisions and reviews that have given numerous insights for other nations in their efforts to regulate cybercrimes.

---

[7] *サイバー警察局とは (About the Cyber Affairs Bureau)*. NPA, https://www.npa.go.jp/bureau/cyber/what-we-do/about.html; A literal translation of the Japanese word "*サイバー事案*" into English is a "cyber affair," which may be an unusual definition of cybercrime.

First, I will review the CFAA and introduce some arguments and important court decisions, such as *Van Buren v. United States*, in the chapters, "History of the CFAA" and "Overview of the Current CFAA." Because the CFAA has nearly 40 years of history, it is important to review its expansion of the subject of the law and its improvement over the decades. In terms of *Van Buren v. United States*, the Supreme Court made an important decision on how to interpret "without authorization" and "exceed authorization." In *Van Buren,* The Supreme Court clarified how we should understand sentences or words in the statutes whose definitions are not clarified in the law. All of this is providing Japanese authorities with insightful considerations of how they might develop and enhance their legal framework for investigating cybercrimes.

Second, I will make a comparison between the CFAA and the Japanese statutes and try to tease out implications from the CFAA in the chapters, "The Japanese Statutes of Cybercrime Regulation" and "Comparison Between the CFAA and Japanese Laws." For cybercrime investigation, Japanese law enforcement has primarily two laws, i.e., the Penal Code (Act No. 45 of 1907) and the Act on Prohibition of Unauthorized Computer Access (Act No. 128 of 1999) (APUCA). I will show details of both laws related to investigating cybercriminals and compare them to the CFAA from the viewpoints of characteristics, objects of regulation, penalties, etc. Overall, there are no huge differences between the CFAA and the Japanese laws in terms of activities that could be illegal, but some slight differences exist, and these might cause some problems for cooperation between the U.S. authorities and those of Japan. It is not only a problem in U.S.-Japan cooperation, but it has also been shown that there are few cases of Japanese authorities cooperating the international cybercrime investigations.

Finally, I will introduce some issues related to cracking down on cybercrimes in the chapter "Unclear Legal Issues." In this paper, I will describe issues such as understanding of authorization, hacking back, and honeypots specifically. Both the United States and Japan are struggling to find a fair way to address these issues, and answers are still unclear. In conclusion, I consider that the role of the CFAA will be shrinking while its significance remains crucial. The situation in Japan, at least the legal framework itself, is not much behind that in the United States. The lack of accumulation of court decisions, however, might make it difficult to enhance the legal framework of cybercrime investigation in Japan. Thus, Japanese authorities could learn from the situation of the United States.

History of the CFAA

Birth of the CFAA

The original form of the CFAA, the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 (CACFAA), was enacted in 1984. At that time, the text of the CFAA was narrow in scope. Some commentators have noted that the movie "WarGames" (1983)[8] was the impetus for enactment,[9] but it was also said that, as of 1983, about 21 states had some form of computer crime legislation in place,[10] suggesting that there was already a considerable amount of interest on the part of lawmakers in the issue. By 1999, all states had some form of cybercrime

---

[8] *WarGames*. Directed by John Badham. MGM, 1983.
[9] Greg Pollaro, "Disloyal Computer Use and the Computer Fraud and Abuse Act: Narrowing the Scope," *Duke Law & Technology Review*, vol. 9, 2010-2011, pp. [1]-[11].
[10] United States Congress House Committee on the Judiciary Subcommittee on Civil and Constitutional Rights. *Computer Crime: Hearing Before the Subcommittee on Civil and Constitutional Rights of the Committee on the Judiciary, House of Representatives, Ninety-Eighth Congress, First Session ... November 18, 1983*. U.S. Government Printing Office, 1984: 2, https://books.google.com/books?id=G0nRxQEACAAJ; Statement of Rep. William Nelson.

statutes.[11] Specifically, the acts prohibited by law were, knowingly without access authorization, or in excess of the scope of the authorization for access granted, (1) stealing a secret from a federal government computer, such as one relating to national security; (2) stealing from a financial institution computer certain important personal information of a customer; or (3) knowingly and without authority, using, modifying, destroying or disclosing information on a federal government computer, or preventing authorized use.[12] Before the enactment of CACFAA, prosecutors and law enforcement agencies struggled to bring cases using traditional criminal statutes. In this sense, CACFAA focused on computer usage and criminalized certain acts involving using computers, which was a historic event in the cybercriminal world. Upon enactment of CACFAA, the Secret Service was given CACFAA investigative authority. In the United States today, the Federal Bureau of Investigation (FBI) and the Secret Service are the primary law enforcement agencies for cybercrime investigations, a foundation that dates back to 1984.

The enactment of the original CFAA was one of the most historical signs of progress in the fight against cybercrimes. There was a tremendous number of complaints by prosecutors, federal and state law enforcement officials, and even lawmakers about this law, however.[13]

---

[11] Orin S. Kerr, 'Cybercrime's Scope: Interpreting Access and Authorization in Computer Misuse Statutes', *New York University Law Review*, 78.5 (2003): 1597.
[12] Ellen S Podgor. "Counterfeit Access Device and Computer Fraud and Abuse Act of 1984." *Major Acts of Congress*, vol. 1, 2004, pp.194-97.
[13] Joseph B. Jr. Tompkins and Linda A. Mar. "The 1984 Federal Computer Crime Statute: A Partial Answer to a Pervasive Problem." *Computer/Law Journal*, vol. 6, no. 3, Winter 1986, pp. 459-84.; Joseph B. Jr. Tompkins and Frederick S. Ansell. "Computer Crime: Keeping up with High Tech Criminals." *Criminal Justice*, vol. 1, no. 4, Winter 1987, pp. 31-46.; *Computer fraud legislation : Hearing before the Subcommittee on Criminal Law of the Committee on the Judiciary, United States Senate, Ninety-ninth Congress, first session, on S. 440 .. and S. 1678 .. October 30, 1985. . , . HeinOnline*, https://heinonline-org.ezp-prod1.hul.harvard.edu/HOL/P?h=hein.cbhear/cmpfrudle0001&i=1.

Taking into account these criticisms, congressional supporters introduced additional bills[14] and made the CFAA[15] to respond to these criticisms.

First radical amendment – 1986

The problem of CACFAA mostly arose from its particularly narrow scope of criminalizing computer misuse and its lack of definitions of terms, such as "without authorization," "access," and "use."[16] For example, from federal law enforcement officials' point of view, CAFAA was difficult to use, and they thought it should be expanded.

Congress responded to the critics by amending CAFAA and enacting the CFAA, and then the statutes of the CFAA became more useful for law enforcement officials than those of the CACFAA.[17] There were two types of amendments: modification of the provisions and the addition of new provisions. The former made the provisions clearer, and the latter expanded the objects of computer misuse.[18]

---

[14] *The Computer Fraud and Abuse Act of 1986. Hearing before the Committee on the Judiciary, United States Senate, Ninety-Ninth Congress, Second Session on S.2281, a Bill To Amend Title 18, United States Code, To Provide Additional Penalties for Fraud and Related Activities in Connection with Access Devices and Computers, and for Other Purposes*. Superintendent of Documents, U, 16 Apr. 1986. *ERIC*, https://eric.ed.gov/?id=ED282520.
[15] Office of the Federal Register, National Archives and Records Administration. 100 Stat. 1213 - Computer Fraud and Abuse Act of 1986. U.S. Government Publishing Office, https://www.govinfo.gov/app/details/STATUTE-100/STATUTE-100-Pg1213.
[16] Office of the Federal Register, National Archives and Records Administration. 98 Stat. 1837 - Acquisition of Foreign Evidence Improvements Act. U.S. Government Publishing Office: 98 Stat. 2190, https://www.govinfo.gov/app/details/STATUTE-98/STATUTE-98-Pg1837.
[17] *The Computer Fraud and Abuse Act of 1986. Hearing before the Committee on the Judiciary, United States Senate, Ninety-Ninth Congress, Second Session on S.2281, a Bill To Amend Title 18, United States Code, To Provide Additional Penalties for Fraud and Related Activities in Connection with Access Devices and Computers, and for Other Purposes*. Superintendent of Documents, U, 16 Apr. 1986. *ERIC*, https://eric.ed.gov/?id=ED282520.
[18] Dodd S. Griffith. "The Computer Fraud and Abuse Act of 1986: A Measured Response to a Growing Problem" *Vanderbilt Law Review*, vol. 43, no. 2, March 1990, pp. 453-90.

The result of the amendments was that they eliminated vague phrases, modified the statute's structures, defined additional words, and widened the range of crime involving computer misconduct. Since the CACFAA had started with a strictly narrow range of objects, these amendments ought to be evaluated as radical.

Expansion of the CFAA in 1994 and 1996

In 1994, the CFAA was amended by section 290001 of the Violent Crime Control and Law Enforcement Act of 1994,[19] which was called the Computer Abuse Amendments Act of 1994, and it added to the CFAA a civil provision to allow victims to recover their damages.[20] In addition to that, its amendments also expanded the scope of the computer damage statute of the CFAA. After this, in 1996, there was a further expansion made by Title II of the Economic Espionage Act of 1996 in three ways.[21] First, it enlarged the scope of information of financial institutions, card issuers, or consumer reporting agencies subject to the protection of the CFAA to include any information obtained by interstate or foreign communication. Second, it added new provisions for computer misconduct and a new felony enhancement. For instance, as for new provisions, a computer extortion statute as well as additional factors to calculate the harm were added to the CFAA. Last, it replaced the "federal interest" category with "protected"

---

[19] Office of the Federal Register, National Archives and Records Administration. 108 Stat. 1796 - Anti-Corruption Act of 1993. U.S. Government Printing Office: 108 Stat. 2097, https://www.govinfo.gov/app/details/STATUTE-108/STATUTE-108-Pg1796.

[20] Orin S. Kerr, "Vagueness Challenges to the Computer Fraud and Abuse Act" *Minnesota Law Review*, vol.94, no.5, May 2010, pp.1561-1587.

[21] Office of the Federal Register, National Archives and Records Administration. 110 Stat. 3488 - National Information Infrastructure Protection Act of 1996. U.S. Government Printing Office: 110 Stat. 3491, https://www.govinfo.gov/app/details/STATUTE-110/STATUTE-110-Pg3488.

computers. This was a kind of renewal of the statutes, but this change dramatically broadened the scope of the statute.[22]

Amendment by the USA PATRIOT Act of 2001

After the terrorist attacks of September 11, 2001, the U.S. Congress passed the USA Patriot Act of 2001.[23] This act included provisions expanding the range of the CFAA as well. One of the most remarkable amendments was to expand the definition of "protected computer." Before this, "protected computer" was only a computer located within the territory of the United States. But now, it includes computers located outside the United States as well.

Amendment by the Identity Theft Enforcement and Restitution Act of 2008

This act was also to widen the scope of the CFAA.[24] First, it expanded the targets of the CFAA prohibiting stealing of information from financial institutions. Originally, the CFAA only targeted such action "if the conduct involved an interstate or foreign communication," but the amendment by the Identity Theft Enforcement and Restitution Act removed this requirement and expanded the scope of the criminal act under the statute. Additionally, it also widened the range of the statute related to causing damage. Finally, it modified the definition of "protected computer" to include any computer.

---

[22] Orin S. Kerr. "Vagueness Challenges to the Computer Fraud and Abuse Act" *Minnesota Law Review*, vol.94, no.5, May 2010, pp.1561-87.
[23] Office of the Federal Register, National Archives and Records Administration. Public Law 107 - 56 - Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001. U.S. Government Printing Office, 25 Oct 2001: 115 Stat. 383, https://www.govinfo.gov/app/details/PLAW-107publ56.
[24] Office of the Federal Register, National Archives and Records Administration. Public Law 110 - 326 - An act to amend title 18, United States Code, to provide secret service protection to former Vice Presidents, and for other purposes. U.S. Government Printing Office, 25 Sep 2008: 122 Stat. 3561, https://www.govinfo.gov/app/details/PLAW-110publ326.

Amendment Defending the Integrity of Voting Systems Act of 2020

This amendment expanded the definition of "protected computer" to include the voting system.[25] In 2018, the Department of Justice (DOJ) issued "The Report of the Attorney General's Cyber Digital Task Force," which concluded that certain types of computers constituting election systems were not protected by the CFAA.[26] Considering the report, Congress passed the amendment that expanded the definition of "protected computer" to include a computer that is part of a voting system regardless of whether it is online or offline.[27] According to the report, the CFAA was not effectively prohibiting hacking into a voting system, although such conduct could constitute other criminal offenses. In this sense, this amendment was designed to close a hole in the CFAA.[28]

Overview of the current CFAA

Characteristics of the CFAA

The CFAA can be used not only for criminal offenses, but for civil cases as well. There are some limitations, however, private entities can seek court decisions and settlements based on the CFAA.[29] Although civil cases tend to occur between a private company and a former employee, they contribute to the accumulation of court decisions. Also, however, the nature of

---

[25] Office of the Federal Register, National Archives and Records Administration. Public Law 116 - 179 - Defending the Integrity of Voting Systems Act. U.S. Government Publishing Office, 19 Oct 2020: 134 Stat. 855, https://www.govinfo.gov/app/details/PLAW-116publ179.
[26] Office of the Deputy Attorney General. *Report of the Attorney General's Cyber Digital Task Force*. DOJ, July 2018: 121, www.justice.gov/archives/ag/page/1076696/download.
[27] 18 USC 1030 (e)(2)(c)
[28] "Congressional Record." *Congress.gov*, Library of Congress, 22 May 2023, https://www.congress.gov/congressional-record/volume-166/issue-163/house-section/article/H4581-1
[29] 18 USC 1030(g).

the CFAA, which applies to civil cases as well, allows local law enforcement agencies to use the CFAA as a basis for investigation and authorizes state Attorneys General to file civil lawsuits.[30]

Illegal acts under the CFAA

According to the statutes, seven types of acts[31] are illegal under the CFAA:[32]

- Cyber Espionage, 18 USC 1030(a)(1);
- Obtaining Information by Unauthorized Access, 18 USC 1030(a)(2);
- Government Computer Trespassing, 18 USC 1030(a)(3);
- Computer Fraud, 18 USC 1030(a)(4);
- Damaging a Computer: Cyber Attack, 18 USC 1030(a)(5);
- Password Trafficking, 18 USC 1030(a)(6);
- Cyber Threatening and Extortion, 18 USC 1030(a)(7).

The CFAA also prohibits an attempt to commit the criminal activities listed above.[33] Because of its wide reach, the CFAA is the main legislation concerning criminal acts and regulating cyber behaviors.

---

[30] McKay Cunningham. *Cyber Law in the United States of America.* Kluwer Law International, 2020: 252

[31] Charles Doyle. *Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws*. Federation of American Scientists, 15 Oct. 2014. *ProQuest*, https://www.proquest.com/docview/1820784447?parentSessionId=hGPY10D5yiPhH6usQKYxo2knlfvsJNcV2oVrF1AYxXg%3D&pq-origsite=primo&; H. Marshall Jarrett, et al. *Prosecuting Computer Crimes*. Office of Legal Education Executive Office for United States Attorneys, 2010: www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf; Macon Bianucci, et al. "Computer Crimes." *American Criminal Law Review*, vol. 59, no. 3, Summer 2022, pp. 511-570. *HeinOnline*, https://heinonline-org.ezp-prod1.hul.harvard.edu/HOL/P?h=hein.journals/amcrimlr59&i=527; I wrote this part of the paper relying heavily on these references.

[32] 18 USC 1030(a).

The specific feature of paragraph 1030(a)(1) is connecting espionage with computer abuse. Although similar to existing espionage laws, this is a significant difference. To charge a person with this crime, there must be evidence that he or she knowingly hacked into a government computer.

Paragraph 1030(a)(2) does not just prohibit hacking activities, but bans obtaining certain protected information from a "protected computer" by unauthorized access. This provision mainly covers information protected by the federal government and financial institutions. It also covers information acquired through interstate or foreign access and information protected by a voting system.

Paragraph 1030(a)(3) prohibits "hacking" into federal government computers and also prevents attempts to do so in subsection 1030(b). Under this article, the mere act of breaking into a federal computer is also treated as a crime.

Paragraph 1030(a)(4) is a provision for criminalizing fraudulent activity by computer intrusion. The statute requires a suspect to have the intent to defraud and acquire anything of value or obtain usage of a computer for more than a minimal amount of $5,000 per year.

Paragraph 1030(a)(5) intends to crack down on causing harm to a computer. Hackers or the creators of malicious programs are targeted by this statute. The 2008 amendments expanded the scope of damages from the previous five categories, which are now factors that are taken into account when determining the penalty. Not only so-called hacking but also denial-of-service

---

[33] 18 USC 1030(b).

(DDoS) attacks[34] and other activities that do not necessarily require breaking into the target computer are subject to the crackdown.

Paragraph 1030(a)(6) was enacted in response to the practice of hackers posting stolen passwords on electronic bulletin boards. This provision is similar to paragraph 1029(a)(2)[35] to ban a certain act, but it has some additional advantages.

Paragraph 1030(a)(7) prohibits attempts to extort money by transmitting communications that might cause damage to the computer itself or data stored on the computer. This clause was added because other laws prohibited extortion, but it was not clear whether extortion by harming a computer or the data stored in it could be prohibited. Cybercrimes committed by ransomware[36] usually violate this article.[37]

"Computer" and "Protected Computers"

The term "computer" used in the CFAA means "an electronic, magnetic, optical, electrochemical, or other high-speed data-processing device performing logical, arithmetic, or

---

[34] DDoS is an abbreviation for Distributed Denial of Service, a type of cyber-attack in which a computer or network is subjected to an intensive load for an extremely short period, thereby disrupting the use of that computer or network. It can be carried out using vulnerable IoT devices, for example.

[35] "Whoever… knowingly and with intent to defraud traffics in or uses one or more unauthorized access devices during any one-year period, and by such conduct obtains anything of value aggregating $1,000 or more during that period… shall, if the offense affects interstate or foreign commerce, be punished as provided in subsection (c) of this section." 18 USC 1029(a)(2).

[36] Ransomware is a term coined by combining the words "Ransom" which means ransom and "Software," and refers to malware that makes files unusable by encrypting them and then demands money, or ransom, in exchange for restoring the files. In 2017, WannaCry, a type of ransomware, infected computers around the world, causing massive damage: several companies were forced to shut down their factories due to infection by WannaCry. For example, in the United Kingdom, the National Health Service, a state-run health service, was affected, resulting in the cancellation of surgeries and the inability to provide medical care.

[37] Peter G. Berris. *Ransomware and Federal Law: Cybercrime and Cybersecurity*. Congressional Research Service, 2021: 3, https://crsreports.congress.gov/product/pdf/R/R46932.

storage functions, and includes any data storage or communications facility directly related to or operating in conjunction with such a device, but the term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar devices."[38] This definition includes almost every device existing in the real world, except for a very simple calculator or a typewriter. The broad definition of "computer" enables law enforcement authorities to investigate state-of-the-art cybercrime by applying the CFAA statutes. The broad definition of "computer" might be considered problematic, in that law enforcement authorities are able to apply statutes to various types of acts intentionally. The definition of "computer," however, is not the sole element that makes a certain type of conduct a cybercrime, so it is not a major issue.[39] Besides "computer," the CFAA defines the term "protected computer"[40] as well. Several provisions[41] within the CFAA specifically relate to "protected computer" and make it one of the factors in determining whether an act is illicit or not. In short, the meaning of "protected computer" is a computer for a financial institution or the U.S. Government, related to interstate or foreign commerce or communication, or part of a voting system used in a federal election. A device connected to the internet including an internet of things (IoT) device is protected under the CFAA based on its definition of "protected computer."

"Without authorization" and "Exceeds authorized access"

No one will be prosecuted under the CFAA provisions if their act is within their access authorization. In this sense, the definition of "access" or "authorization" is important. In the

[38] 18 USC 1030(e)(1).
[39] Jonathan Clough. *Principles of Cybercrime*. Cambridge University Press. 2010: 52.
[40] 18 USC 1030(e)(2).
[41] 18 USC 1030(a)(2)(c), 1030(a)(4), 1030(a)(5), 1030(a)(7).

CFAA, however, only "exceeds authorized access" has a definition and it contains the undefined phrase "with authorization" in its provision, which makes the definition of "exceeds authorized access" incomplete. This lack of definition has been particularly problematic when a defendant who has damaged a computer is an insider and has a kind of access authorization. Without a Supreme Court decision, the interpretation of "access" or "authorization" has been divided among circuit courts for decades. In 2021, the Supreme Court made the first decision on the meaning of "access."[42] Until then, there were two interpretations of "authorization": a narrow interpretation based on a technical perspective and a broad interpretation based on contracts and circumstances, but at least in the case of *Van Buren v. United States*,[43] the Supreme Court decided the "narrow" interpretation was correct. This interpretation would seem to be unjustified, at least from the standpoint of the investigator.

In *Van Buren v. United States*, the Supreme Court presented an interpretation of "access" by analyzing the word "so" in the definition of "exceeds authorization" to decide whether the defendant was guilty or not. They found that Van Buren violated the CFAA. In everyday life, it seems natural to make a judgment on whether a behavior exceeds its authorization based on all the circumstances. The Supreme Court, however, used a narrow interpretation in *Van Buren v. United States*, emphasizing that it is only a statute of law and that the CFAA specifically

---

[42] United States, Supreme Court. *Van Buren v. United States*. 3 June 2021. *Legal Information Institute*, Cornell U Law School, https://www.law.cornell.edu/supremecourt/text/19-783.

[43] Former Georgia police sergeant Nathan Van Buren used his patrol-car computer to access a law enforcement database to retrieve information about a particular license plate number in exchange for money. Although Van Buren used his valid credentials to perform the search, his conduct violated a department policy against obtaining database information for non-law-enforcement purposes. Unbeknownst to Van Buren, his actions were part of a Federal Bureau of Investigation sting operation. Van Buren was charged with a felony violation of the Computer Fraud and Abuse Act of 1986 (CFAA), which subjects to criminal liability anyone who "intentionally accesses a computer without authorization or exceeds authorized access."

regulates cybercrime. According to the Supreme Court opinion, "access" means "the act of entering a computer 'system itself' or a particular 'part of a computer system,' such as files, folders, or databases."[44] This opinion was reached after consulting dictionaries of computer technology. This meaning of "access" is extremely clear if you can assume a computer system is a house and a part of a computer system is a room. Criminal statutes should have a clear definition so as not to punish a person who should not be punished because a criminal penalty is one of the most invasive measures to limit human rights that the government can impose on people. In this way, the decision of the Supreme Court was understandable. On the other hand, it would be natural for one to understand that a certain file, folder, or database requires a user to have access authorization to each; however, it would be difficult to assume what "exceeds authorization" is. It can be believed that the decision of the Supreme Court provides the meaning of "authorization" in the context of the CFAA.[45] Based on the understanding of *Van Buren v. United States*, access authorization is confined technically and seems to have a clear boundary for its authorization. In this sense, I consider "exceeds access authorization" to have no meaning.

The Japanese statutes of cybercrime regulation

Overview

There are two main vehicles used to crack down on cybercrime in Japan: the Penal Code and APUCA. Although the Penal Code is a general criminal statute, of which cybercrimes are just a part, it is sufficient to punish cybercrime suspects. In Japanese law, the word "electronic

[44] United States, Supreme Court. *Van Buren v. United States*. 3 June 2021. *Legal Information Institute*, Cornell Law School, https://www.law.cornell.edu/supremecourt/text/19-783.
[45] Orin S. Kerr. "Focusing the CFAA in Van Buren" *The Supreme Court Review*, vol. 2021, 2021, pp.155–84.

calculator" *電子計算機* is used to mean "computer,"[46] but neither the Penal Code nor APUCA has an article defining the term. The definition of "electronic calculator" – or computer - is not clearly defined in the law, but whether or not it is a covered computer is to be determined based in the text of the respective law. Although there is no definitive interpretation based on case law, it is generally believed that electronic devices that merely perform calculations and data processing, such as calculators and electronic dictionaries, do not constitute "electronic calculators" in some statutes.[47]

According to a report from the National Police Agency of Japan (NAP),[48] the number of cybercrimes, including crimes involving the internet, has been increasing. Reviewing the report, most cybercrimes recognized by Japanese police are network-enabled crimes, but in this section, I am going to focus on the Penal Code and APUCA, which prohibit cybercrime targeting the computer itself and interprets using a computer as part of a crime.

Penal code

There are some articles in the Criminal Code that apply to cybercrime. In particular, those targeting computers themselves are Articles 161-2,[49] 168-2,[50] 168-3,[51] 234-2,[52] and 246-2[53] of

---

[46] Other than the Penal Code and APUCA, it is also used in many other laws, such as the Civil Code (Act No. 89 of 1896), the Consumer Contract Act (Act No. 61 of 2000), and the Banking Act (Act No. 59 of 1981).

[47] Otsuka, Hitoshi, et al. *大コンメンタール刑法[第三版]第12巻 (Grande Commentaire Criminal Law [3rd ed.], Vol. 12).* Seirin-Shoin, 2019: 249.

[48] *令和４年版警察白書 (The White Paper on Police 2022)*. NPA, 2022, https://www.npa.go.jp/hakusyo/r04/index.html.; *令和３年におけるサイバー空間をめぐる脅威の情勢等について (Threats Related to Cyber Space in 2021)*. NPA, Apr. 2022, www.npa.go.jp/publications/statistics/cybersecurity/data/R03_cyber_jousei.pdf.

[49] (Unauthorized Creation of Electronic or Magnetic Records)
Article 161-2 (1) With the intent to bring about error in the processing of matters of another person, a person who unlawfully creates an electronic or magnetic record without due authorization which is for use in such

the Penal Code.[54] Articles 161-2, 234-2, and 246-2 were added in 1987,[55] and Articles 168-2 and 168-3[56] were added in 2011. The amendment of 1987 was to deal with a crime that was

---

improper processing and is related to rights, duties or certification of facts, is punished by imprisonment for not more than 5 years or a fine of not more than ¥500,000.

(2) When the crime prescribed under the preceding paragraph is committed in relation to an electronic or magnetic record to be created by a public office or a public employee, the offender is punished by imprisonment for not more than ten years or a fine of not more than ¥1,000,000 yen is imposed.

(3) A person who, with the intent prescribed in paragraph (1), puts an electronic or magnetic record created without due authorization and related to rights, duties or certification of facts into use for the processing of matters of another person is punished by the same penalty as the person who created such an electronic or magnetic record.

(4) Any attempt to commit the crimes prescribed under the preceding paragraph is punished.

[50] Making of Electronic or Magnetic Records Containing Unauthorized Commands

Article 168-2 (1) A person who, without legitimate grounds, creates or provides any of the following records including electronic or magnetic records for the purpose of using them for executing commands on another person's computer is punished by imprisonment for not more than 3 years or a fine of not more than ¥500,000 yen:

(i) electronic or magnetic records that give unauthorized commands to prevent a computer from performing functions in line with the user's intention or have it perform functions against the user's intention;

(ii) beyond what is set forth in the preceding item, records including electronic or magnetic records in which unauthorized commands referred to in the same item are described.

(2) The same applies to a person who, without legitimate grounds, uses electronic or magnetic records set forth in item (i) of the preceding paragraph for the execution of commands on another person's computer.

(3) Any attempt to commit the crime referred to in the preceding paragraph is punished.

[51] Acquisition of Electronic or Magnetic Records Containing Unauthorized Commands

Article 168-3 A person who, without legitimate grounds, acquires or stores records including electronic or magnetic records set forth in the items of paragraph (1) of the preceding Article for the purpose referred to in the same paragraph is punished by imprisonment for not more than 2 years or a fine of not more than 300,000 yen.

[52] Obstruction of Business by Damaging a Computer

Article 234-2 (1) A person who obstructs the business of another person by interfering with the operation of a computer utilized for the business of the other or by causing such computer to operate counter to the purpose of such utilization by damaging such computer or any electronic or magnetic record used by such computer, by inputting false data or giving unauthorized commands or by any other means, is punished by imprisonment for not more than 5 years or a fine of not more than ¥1,000,000].

(2) Any attempt to commit the crime prescribed under the preceding paragraph is punished.

[53] Computer Fraud

Article 246-2 Beyond what are provided for in the provisions of the preceding Article, a person who illegally obtains or causes another person to illegally obtain a profit by creating a false electronic or magnetic record relating to acquisition, loss, or alteration of property rights by inputting false data or giving unauthorized commands to a computer utilized for the business processes of another person, or by putting a false electronic or magnetic record relating to acquisition, loss, or alteration of property rights into use for the business processes of another person, is punished by imprisonment for not more than ten years.

[54] *国民のためのサイバーセキュリティサイト (Cybersecurity website for nationals)*, Ministry of Internal Affairs and Communications, https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/basic/basic_legal_02.html.

[55] *刑法等の一部を改正する法律(昭和 62 年 6 月 2 日法律第 52 号) (Act for Partial Revision of the Penal Code, etc. (Act No. 52 of June 2, 1987)).*

committed by using a computer in the context of the rapid spread of computers. The Penal Code was not always applicable to such a crime before the revision; therefore, this amendment added to the new provisions specified in computer misuse. It was not the amendment that created the new type of crime, but modified statutes for punishing traditional crime when conducted via computer, even though the amendment added new provisions to the Penal Code when it comes to the substantial meaning. On the other hand, the amendment of 2011 was a substantial revision that created new types of crimes, which are so-called "computer virus-related crimes." This amendment, along with the revision of APUCA, was implemented not only for dealing with emerging situations but also in order to conclude the Convention on Cybercrime, which mandates that prospective member countries criminalize specific acts of computer misuse.[57] As I have mentioned, the Penal Code now makes it illegal to use a computer to forge documents, obstruct business, commit fraud, and commit acts related to computer viruses. In 2021, the number of criminal cases cleared under the cybercrime provisions of the Penal Code exceeded that of 2020, with 729 cases.[58]

In the Penal code, the acts listed below are prohibited.

---

[56] *"情報処理の高度化等に対処するための刑法等の一部を改正する法律(平成23年6月24日法律第74号)(Act for Partial Revision of the Penal Code, etc. to Cope with Advanced Information Processing, etc. (Act No. 74 of June 24, 2011)).*
[57] 177th Diet Session, House of Representatives, Committee on Judicial Affairs, No. 13, May 25, 2011, Statement of Purpose of the Act for Partial Revision of the Penal Code, etc. to Cope with Advanced Information Processing, etc., https://www.shugiin.go.jp/internet/itdb_kaigirokua.nsf/html/kaigirokua/000417720110525013.htm.
[58] *犯罪統計 (Crime Statistics)*, NPA, https://www.npa.go.jp/publications/statistics/sousa/statistics.html.

- **Article 161-2: Unauthorized Creation of Electronic or Magnetic Records**

Originally, the forgery of official and private documents was prohibited by the Penal Code,[59] but there was disagreement as to whether electromagnetic records constituted "documents" or not. As electromagnetic records became more prevalent, however, the evidentiary function of electromagnetic records became more important, so they were newly added in 1987 to provide the same level of protection as official and private documents. The Japanese Supreme Court's decision on this article was issued in 2021 in the so-called Mt. Gox case, which occurred in 2014.[60] This case concerned crypto assets. As for Article 161-2 of the Penal Code, the defendant was the sole decision-maker in the company, and the issue was whether the defendant created the electromagnetic record of the balance of the crypto assets "against the will of the company" and, if so, whether his actions that created the electromagnetic record were "unlawful." There are many issues in dispute; however, in this case, it is interesting to note that the lower courts and the Appellate court have consistently recognized that the defendant's violation of Article 168-2 of the Penal Code is established. Although the text of the articles and the background of the case are different, in contrast to the *Van Buren v. United States*, which was decided based on the extent to which access privileges were technically restricted, the Mt. Gox case also considered the impact of

[59] Penal Code; Chapter XVII Crimes of Counterfeiting of Documents.
[60] Supreme Court of Japan Decision on January 27, 2021; Tokyo High Court Decision on June 11, 2020; Tokyo District Court Decision on March 15, 2019; The Supreme Court decided to dismiss the appeal simply because it did not fall within the grounds for appeal.

the system on the users and the terms of use, all of which led to the conviction of the defendant.

- **Article 168-2: Making of Electronic or Magnetic Records Containing Unauthorized Commands**
- **Article 168-3: Acquisition of Electronic or Magnetic Records Containing Unauthorized Commands**

These articles were added by the 2011 amendment. Before this, the mere creation or possession of a malicious program, such as malware, was not punishable. This amendment was necessary not only to ensure public confidence in the internet and computers, but also to fulfill obligations under the Cybercrime Convention. Both Article 168-2 and Article 168-3 make "without legitimate grounds" a requirement for the commission of a crime. This requirement exists to make it clear that no crime is committed, for example, when malware is possessed for the development or testing of antivirus software.

- **Article 234-2: Obstruction of Business by Damaging a Computer**

The act of "obstruction of business," which was originally considered illegal under the Penal Code,[61] was an act intended to be committed against a business conducted by a person. As such, the elements of the crime included the means or methods of

[61] Articles 233 (Damage to Credibility; Obstruction of Business) and 234 (Forcible Obstruction of Business).

influencing a person's will or behavior. There are, however, some acts of obstruction committed against computers that do not necessarily affect "a person's will or actions," but that, as a result, cause obstruction of business. This article contains roughly three elements: 1) corruption of a computer or its data, or giving false information or unauthorized instructions; 2) causing the computer in question to malfunction; 3) then, if the malfunctioning interferes with the business of others, it will constitute an act prohibited by the Penal Code. This crime carries a heavier penalty, both in terms of imprisonment and fines, than the traditional obstruction of business crime.[62] This is in consideration of the fact that obstruction of business against a computer can have a greater impact on society as a whole than traditional obstruction of business.[63]

- **Article 246-2: Computer Fraud**

This article was originally added to the Penal Code after counterfeit phone cards became a major social problem in the 1980s.[64] The problem was that when what is stolen is data, it is not a physical object and therefore not punishable under ordinary theft charges,[65] while fraud is not punishable under ordinary fraud charges[66] because

[62] The penalties under Articles 233 and 234 of the Penal Code are imprisonment for not more than three years or a fine of not more than ¥500,000. On the other hand, the penalty under Article 234-2 of the Penal Code is imprisonment for not more than five years or a fine of not more than ¥1,000,000.
[63] Otsuka, Hitoshi, et al. *大コンメンタール刑法[第三版]第12巻 (Grande Commentaire Criminal Law [3rd ed.], Vol. 12)*. Seirin-Shoin, 2019: 246-247.
[64] Regarding the issue of counterfeit telephone cards, the Supreme Court of Japan has decided that telephone cards are securities under the Penal Code, and altering a telephone card is punishable as counterfeiting security.
[65] Article 235 (Theft).
[66] Article 246 (Fraud).

> it cannot be committed without an act of "deceiving" a person. Therefore, it was necessary to make it possible to punish the act of manipulating computers and data for financial gain. There are two acts that are punishable under this article. One is the act of creating false information by using a computer for financial gain, and the other is the act of using already existing false information for financial gain. This makes it a punishable offense, for example, if a suspect accesses a server computer of a bank that maintains information on customers' bank accounts, fraudulently changes the balance of an account, withdraws money from an ATM, and obtains a financial benefit unlawfully. Without this article, this act might be neither theft nor fraud, according to the detailed interpretation of the article.

Act on Prohibition of Unauthorized Computer Access

As we have seen in the Penal Code section, interest in cybercrime itself has existed in Japan since 1987, but there was no law prohibiting the act of so-called "unauthorized access" per se. This not only meant that cybercrime countermeasures in Japan lagged behind the rest of the world. Cybercrimes are committed using the internet, regardless of national borders. While countries around the world were working together to combat cybercrime, Japan's lack of a law prohibiting cybercrime was a major problem from the perspective of international cooperation. This is because, under Japan's criminal law system, it is not possible to cooperate with a request for help in the investigation of a crime from a foreign country unless that crime is also considered a crime in Japan.[67] In 1999, in light of the international situation described above,

[67] Article 2 This Code applies to anyone who commits one of the following crimes outside the territory of Japan:

and in order to prevent "unauthorized access" that cannot be addressed by the Penal Code or other laws alone, APUCA[68] was passed by the Diet and enacted in 2000. After APUCA went into effect in 2000, the importance of safeguarding the internet continued to grow. There was also an increase in cybercrime and the amount of damage caused, as well as a serious incident in which the IDs and passwords for the official computers of members of the Diet may have been compromised in a cyberattack. There was also a problem of an increase in cybercrime due to a sharp increase in so-called "phishing activities," i.e., the act of fraudulently requesting IDs and passwords through fake e-mails or fake websites. Another problem was the absence of

---

(i) deleted;
(ii) the crimes prescribed under Articles 77 through 79 (Insurrection; Preparations; Plots; Accessoryship to Insurrection);
(iii) Crimes described under Articles 81 (Instigation of Foreign Aggression), 82 (Assistance to the Enemy), 87 (Attempts) and 88 (Preparation; Plots);
(iv) the crime prescribed under Article 148 (Counterfeiting of Currency and Uttering Counterfeit Currency) as well as an attempt thereof;
(v) the crimes prescribed under Article 154 (Counterfeiting of Imperial or State Documents), 155 (Counterfeiting of Official Documents), 157 (False Entries in the Original of Notarized Deeds) and 158 (Uttering Counterfeit Official Documents), and the crime concerning an electronic or magnetic record which should be created by a public office or a public employee in Article 161-2 (Unauthorized Creation of Electronic or Magnetic Records);
(vi) the crimes prescribed under Articles 162 (Counterfeiting of Securities) and 163 (Uttering Counterfeit Securities);
(vii) the crimes prescribed under Articles 163-2 through 163-5 (Unauthorized Creation of Payment Cards with an Electronic or Magnetic Record; Possession of Payment Cards with an Unauthorized Electronic or Magnetic Record; Preparation for Unauthorized Creation of Payment Cards with an Electronic or Magnetic Record; Attempts);
(viii) the crimes described under Articles 164 through 166 (Counterfeiting or Unauthorized Use of the Imperial Seal; Counterfeiting or Unauthorized Use of Official Seals; Counterfeiting or Unauthorized Use of Official Marks) as well as any attempts to commit the crimes prescribed under paragraph (2) of Article 164, paragraph (2) of Article 165, and paragraph (2) of Article 166.

[68] 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.

regulations to prevent the illicit distribution of IDs and passwords that had already been leaked.[69] In light of this situation, APUCA was amended in 2012. As a result, phishing and the illicit storage and distribution of other people's IDs and passwords were newly prohibited. In addition, the penalties were strengthened, increasing the maximum penalties for imprisonment and fines.

In APUCA, three types of "acts of unauthorized computer access"[70] are defined and prohibited. The "acts of unauthorized computer access" defined by APUCA are limited to acts committed against network-connected computers with an "access control feature."[71] This network is not limited to the internet, but can be a closed network or a Wi-Fi connection. There are only two types of exceptions to "acts of unauthorized computer access." The first is when the system administrator performs the act, which is objectively unauthorized computer access, such

---

[69] Husei Akusesu Taisaku Housei Kenkyukai. *逐条 不正アクセス行為の禁止等に関する法律［第二版］(Article-by-article Explanation: The Act on the Prohibition of Unauthorized Computer Access 'Second edition').*Tachibana shobo, 2012: 18-19.

[70] Article 2(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. See also Figure 2

[71] Article 2(3); Figure 1.

as when a penetration test is performed to check security, by the system administrator him or herself or by a third party with the consent of the system administrator. The second is when it is performed with the consent of the user who has access authorization. This is assumed to be the case when a parent allows his/her child to use his/her computer.

There are five types of illegal acts in APUCA as well.

- **Article 3: Prohibition of Acts of Unauthorized Computer Access**[72]

  As stated in the article, the article prohibits "any person" from conducting acts of unauthorized computer access. If the act in question constitutes an "act of unauthorized computer access" as defined by APUCA, it is subject to prohibition under this article. Although this may not be consistent with the general sense, only "acts of unauthorized computer access" as defined by APUCA are subject to Article 3. In other words, even if the act of computer access is against the intention of the administrator of a computer that has not been restricted for specific use by access control functions, it is not prohibited by Article 3.

- **Article 4: Prohibition of Acts of Obtaining Someone Else's Identification Code**[73]

  This article was added by the 2012 amendment. This article prohibits acquiring another person's identification code among preparatory acts for unauthorized computer access. The act that is prohibited by this article is the act of obtaining

[72] (Prohibition of Acts of Unauthorized Computer Access)
Article 3 It is prohibited for any person to engage in an act of unauthorized computer access.
[73] (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)).

"another person's" password or ID for the purpose of using it for “unauthorized computer access" as defined in APUCA. The purpose of this article is to ensure the effectiveness of APUCA by prohibiting obtaining identification codes preparatory to unauthorized computer access. This article, coupled with Article 6 of APUCA, prohibits obtaining and storing identification codes of someone else as an element of a series of acts of unauthorized computer access and makes these acts illegal to prevent identification codes from being leaked and circulated.

- **Article 5: Prohibition of Acts of Facilitating Unauthorized Computer Access**[74] This article prohibits the act of providing another person's ID or password to anyone other than the access manager or legitimate user without a legitimate reason, such as being part of the business. The act of providing another person's ID or password is an act that facilitates unauthorized computer access. There are many ways to commit unauthorized computer access, but once IDs and passwords are obtained, it is possible to commit unauthorized computer access without using technically difficult methods. The purpose of this article is to increase the effectiveness of the prohibition of unauthorized computer access activities. This article does not make the subjective requirements of the actor an element of the crime. In addition, the provision of IDs and passwords means that the IDs and passwords are made available to third parties, and the means or method of providing the IDs and passwords does not matter. The

[74] (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.

actor, however, must be aware that he or she is providing another person's identification code to a third party.

- **Article 6: Prohibition of Acts of Wrongfully Storing Someone Else's Identification Code**.[75]

  This article was added by the 2012 amendment, and the main purpose of this article, which prohibits storing someone else's IDs, passwords, or similar information that is the same as Article 4. Based on the purpose of this article, which is to prevent the unlawful distribution of another person's identification code, the subject identification code is limited to those that have been "unauthorizedly obtained." This limitation is intended to ensure that acts subject to punishment are not overly broad. On the other hand, for these "wrongfully obtained" IDs and passwords, the method of acquisition need not be a method that violates Article 4 or Article 5 of APUCA. A detailed interpretation of the text of this article is that a person who keeps the identification code, which is obtained by someone "without legitimate authority," but not limited to an illegal act, for "the purpose of using it to gain unauthorized computer access" is subject to punishment under this article.

[75] (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.

- **Article 7: Prohibition of Acts of Illicitly Requesting the Input of Identification Code**[76]

  This article was added by the 2012 amendment to prohibit so-called "phishing." Phishing is an act that often leads to subsequent fraud and is also frequently used to obtain another person's identification code fraudulently. For these reasons, the act of phishing itself is risky and has been struck down as illegal in and of itself. While there are many different methods of phishing, a common feature is an attempt to deceive a user into believing that the website or e-mail is genuine and to steal the identification code, such as IDs or passwords, by taking advantage of the user's gullibility. APUCA specifically prohibits phishing through the use of websites and e-mail.

APUCA is not only for prohibiting acts of conducting cybercrime, but also for enhancing the ability of private entities to count on cybersecurity with the assistance of public safety

[76] (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.

commissions and the Government of Japan.[77] Considering its nature, it is clear that APUCA is more than just a criminal law to prevent cybercrime. The characteristic of APUCA is also very

[77] (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 the National 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.

clear in Article 1, which defines the Purpose of the Act. The ultimate purpose of APUCA is "contributing to the sound development of an advanced information and telecommunications society."[78]

Comparison between the CFAA and Japanese Laws

Characteristics

The CFAA is used directly in civil court, while the Penal Code and APUCA are not. Of course, in finding a tort, the existence of an illegal act as defined in the articles of the Penal Code or APUCA may be a point of contention in a trial, but it is not a direct basis on which damages or other compensation can be claimed. In addition, in Japan's criminal justice system,[79] indictable cases may result in convictions with little or no contest, and the interpretation of a legal provision is rarely disputed. In that respect, the situation is very different from the accumulation of precedents in the CFAA, which is often contested in civil courts. Of course, even in the United States, there have been few cases challenged in criminal trials,[80] but the accumulation of court cases concerning the CFAA is noteworthy because of its use in civil trials as well.

---

[78] "The purpose of this Act is to prevent computer-related crimes committed via telecommunications lines and maintain telecommunications-related order as realized using 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." Article 1.

[79] It is left to the discretion of the prosecutor to decide whether to indict a suspect in a given case and bring him or her to a criminal court. As a result, most cases that are prosecuted tend to be those in which a guilty verdict is likely to be rendered; according to prosecution statistics for 2021, the prosecution rate of cases by prosecutors was only about 33 percent.

[80] John Gramlich. "Only 2 percent of Federal Criminal Defendants Go to Trial, and Most Who Do Are Found Guilty." *Pew Research Center*, https://www.pewresearch.org/short-reads/2019/06/11/only-2-of-federal-criminal-defendants-go-to-trial-and-most-who-do-are-found-guilty/; Most are convicted through plea bargains without being brought to a criminal trial, and studies of criminal justice in the U.S. also show that most federal criminal offenses result in guilty verdicts.

While the CFAA was originally enacted to prohibit certain computer misuse as a cybercrime from the perspective of protecting critical information of government and financial institutions and preventing interference with their operations, Japan has added new articles to the Penal Code with a view to closing loopholes in the law to effectively prevent business interference and fraud. Legislation criminalizing computer abuse itself as a cybercrime was delayed by about 15 years after the CFAA.

Object

Although it is difficult to simply compare the provisions of the CFAA, the Penal Code and APUCA, most acts considered cybercrime under the CFAA are also treated as cybercrimes in Japan.[81] On the other hand, since there is no article in Japan that directly prohibits cyber espionage, it is only the same as other "unauthorized computer access acts" for investigative agencies to probe.[82]

The computers covered by the provisions of the laws are likely to be more extensive under the CFAA[83] than under the Penal Code or APUCA, by the legal definition of the term. In practice, however, there seems to be no difference in this regard, since most of the computers

[81] Table 1.
[82] For ordinary espionage activities, theft charges under the penal code may be applied if the stolen information is physical, such as documents. If the information falls under the category of trade secrets of a company, a violation of the Unfair Competition Prevention Act (Act No. 47 of 1993) may be established. If a company or a person divulges information about technology that affects so-called international security, it may be charged with violations of the Foreign Exchange and Foreign Trade Act (Act No. 228 of 1949). In addition to that, a person who passed information that is prohibited to be leaked to a "spy" could be charged with the violation of keeping secrets under various laws.
[83] "the term "computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device." 18 USC 1030(e)(1).

covered are those that are used by the general public, such as so-called general-purpose computers and server computers. This point could be the biggest difference between the CFAA and the Japanese legal framework though. In other words, the CFAA may be able to target a wider range of crimes against electronic devices for investigation than the Japanese provisions when particular situations arise. Still, the terms "computer" and "electronic calculator" (*電子計算機*) have the same concerns. This may be the case where the end-to-end encrypted communication network of a communication app, such as WhatsApp, Zoom, FaceTime, etc. is penetrated and its contents are stolen, without penetrating the devices themselves. In the United States, a case related to this problem has already been brought to court.[84] This case is being litigated under the CFAA, and some have argued that a reasonable ruling could be derived by theorizing that the encrypted network itself could be included in the scope of CFAA protection.[85] In other words, the environment surrounding computers has become much more complex than when either law was enacted. In this regard, it is also difficult to interpret the statutes of APUCA in a way that protects the entire system, including the devices connected through the internet, from illegal actions, rather than solely focusing on each individual computer. The object of unauthorized access is only an individual computer.

---

[84] Complaint & Demand for Jury Trial at 1, WhatsApp, Inc. & Facebook, Inc. v. NSO Grp. Technologies Ltd. & Q Cyber Technologies Ltd., No. 3:19-cv-07123, 2015 WL 1033734 (N. D. Cal. Oct. 29, 2019); WhatsApp, Inc. and its parent company Facebook, Inc. filed a lawsuit under the CFAA and California law alleging that NSO Grp. Technologies Ltd. had sent malware to approximately 1,400 mobile devices to covertly monitor their end-to-end encrypted communications.

[85] Jonathon W. Penney and Bruce Schneier. "Platforms, Encryption, and the CFAA: The Case of WhatsApp v. NSO Group." *Berkeley Technology Law Journal*, vol. 36, no. 1, 2021, pp. 469-510.

Exceptions for legitimate acts

In addition, the CFAA clearly stipulates in its text that there is an exception for acts performed by law enforcement and intelligence agencies, while no such special exception exists in the Japanese Penal Code or APUCA. For example, the act of hacking into a suspect's computer for investigation may be considered illegal, since it does not fall under the investigative methods requiring a warrant as stipulated in the Japanese Code of Criminal Procedure. This difference might come from the posture toward methods of criminal investigation in both countries. Although law enforcement officials have to seek the best ways they can take within their country's legal restrictions, Japanese law enforcement, such as prefectural police, is always struggling to find a way to maintain the balance between human rights protection and efficient investigation.

Penalties

The maximum term of imprisonment for first-time offenders in both statutes is generally equivalent to each other in the corresponding provisions. One difference between the CFAA and APUCA, however, may be that under the CFAA, the act of trespassing into a government computer or trafficking a password can be subject to a maximum of 10 years in prison for a second offense. In APUCA, there are no specific provisions for a second-time offender, so judges are sentencing second-time offenders based on the Penal Code's general rule of sentencing when they make a conviction. In any case, due to differences in the way penal laws and regulations determine the extent of punishment, it is possible that the same act could result in different periods of imprisonment in the United States and Japan, but both countries consider cybercrime a serious offense.

Compared to the fines in the Japanese Penal Code and APUCA, the maximum fine for a single violation in the CFAA is U.S.$250,000,[86] which appears to be quite high. Even if one U.S. dollar were converted to an exchange rate of 100 Japanese yen, the maximum fine for a violation of Article 161-2 of the Penal Code is ¥1,000,000, which is the highest maximum fine among the provisions I mentioned to combat cybercrime in Japan, so the fine in the United States could be 25 times higher. Since fines under U.S. federal criminal law are largely at the discretion of the court, simple comparisons cannot be made, but this comparison helps in understanding the overview of the framework.[87]

Miscellaneous

APUCA not only defines acts that constitute a cybercrime but also stipulates the duty of access managers to prevent cybercrime and includes provisions for assistance by the Public Safety Commission and the Japanese government.[88] On the other hand, the CFAA, although

---

[86] 18 USC 3571(b)(3)

[87] Table 2.

[88] (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

used for civil trials, is only a part of the Criminal Code and is the law that defines what acts constitute cybercrimes and what penalties are imposed.

Unclear Legal issues

Unauthorized and Exceeding Authorization

Under APUCA, there is no such thing as "access that exceeds the authorization of access," and "unauthorized access" exists only as a definition, so the CFAA's discussion of "access that exceeds the authorization of access" is not directly at issue.[89] It is only a question of whether or not access control is technically in place when it comes to the interpretation of APUCA. In this sense, the decision in *Van Buren v United States* has an affinity with the interpretation of the text

---

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.

[89] APUCA articles 2 and 3.

of APUCA. APUCA defines “acts of unauthorized computer access” legally by classifying them into three patterns, but they are classified only from a technical perspective. Authorization of access is also considered based on whether the password or ID is held in a valid manner. Therefore, the existence of authorization of access and the scope of authorization of access are rarely linked to issues in the application of APUCA. On the other hand, in criminal law, the presence or absence of “legitimate grounds” and whether or not it is an “unauthorized command” is important in determining whether or not an act is illegal covered by the article. Whether “access exceeding the authorization of access” can be said not to constitute “legitimate grounds” or an “unauthorized command” will have to await the court's decision. A cybercrime committed by, for example, state-sponsored cybercrime groups or a cybercrime committed by outsiders, however, are, by their nature, committed by those who do not have access authorization in the first place. Therefore, from the perspective of cracking down on truly malicious acts, this may not be a very important issue. Of course, in Japan, as in the United States, it is important to consider what the terms of use[90] are and how access is technically controlled since the issue of whether there has been an “act of unauthorized computer access” is often between a company and a retired or fired employee. In any case, this is an issue that needs continued consideration. There is an article that recommends that employers tighten their security restrictions on employees’ system use and does not see policy restrictions as sufficient to bind their use.[91]

---

[90] In considering whether or not to apply criminal laws and regulations, it is necessary to be cautious about taking into account a wide range of circumstances, such as terms of use and implied intentions, as this may make the scope of punishment ambiguous. There is also a possible concern that the terms of use could in effect be used to determine whether or not criminal laws and regulations are applicable.

[91] Emily Chase-Sosnoff and Shane T. Muñoz. “Understanding the Bounds of the Computer Fraud and Abuse Act in the Wake of Van Buren.” *Florida Bar Journal*, vol. 96, no. 2, April. 2022, pp. 22-29.

Hacking back

In the case of Japan, APUCA provides very narrow exceptions, so as a method of investigation, so-called hacking back is considered impossible under the current legal framework. On the other hand, as a general principle of criminal justice, there is room for "justifiable acts,"[92] "self-defense,"[93] and "necessity"[94] to be recognized, so that hacking back by investigative agencies and other organizations can be considered possible even within the current legal framework. Nevertheless, it is an unresolved issue because it has never been challenged in the judiciary and the principle of conduct of the Japanese police rarely allows them to use investigative methods that could amount to illegal acts. For example, the most reliable solution would be to provide for exceptions by law, as in the case of interception of communications. In the United States,[95] legislation has been proposed to enable active cyber defense, but no legislation has been enacted.[96]

---

[92] (Justifiable Acts)
Article 35 An act performed in accordance with laws and regulations or in the pursuit of lawful business is not punishable.

[93] (Self-Defense)
Article 36 (1) An act a person was compelled to take to protect the rights of oneself or any other person against imminent and unlawful infringement is not punishable.
(2) An act exceeding the limits of self-defense may lead to the punishment being reduced or may exculpate the offender in light of the circumstances.

[94] (Necessity)
Article 37 (1) An act a person was compelled to take to avert a present danger to the life, body, liberty or property of oneself or any other person is not punishable only when the harm produced by such act does not exceed the harm to be averted; provided, however, that an act causing excessive harm may lead to the punishment being reduced or may exculpate the offender in light of the circumstances.
(2) The preceding paragraph does not apply to a person under special professional obligation.

[95] Peter G. Berris. *Cybercrime and the Law: Computer Fraud and Abuse Act (CFAA) and the 116th Congress*. Congressional Research Service, 2020.

[96] "H.R.3270 - 116th Congress (2019-2020): Active Cyber Defense Certainty Act." *Congress.gov*, Library of Congress, 28 June 2019, https://www.congress.gov/bill/116th-congress/house-bill/3270.

Honeypots

A honeypot is a computer that intentionally has vulnerabilities to cybercrimes or cyberattacks. By deliberately making that computer the target of hacking, the intent is to identify the perpetrators of the cybercrime or cyberattack and to understand what means they used to do so. A honeypot sometimes includes this act of observation as well. Often, computers that are already victims of cybercrime or cyberattacks are utilized as honeypots. There is also a risk that computers that have been utilized as honeypots may be utilized in cybercrime infrastructures. Even if a computer under one's control is utilized as a honeypot and does not cause damage to other people's computers because of appropriate management, it may still constitute a criminal offense under, for example, the Penal Code's computer virus-related crimes. As for the interpretation of Articles 168-2 and 168-3, if it is for a legitimate purpose such as research, one cannot be charged with a crime, but since there have been no court cases to date, this seems to be a remaining issue. In addition to that, using honeypots may give rise to the question of whether it is similar to wiretapping. If law enforcement officials operate honeypots as an investigation method, it may violate provisions of the procedural law in Japan[97] and constitutional restrictions on the secrecy of any means of communication. Even if it can be done under the restriction of the wiretapping law,[98] the requirements of conducting wiretapping are extremely strict, and there are few cases using wiretapping in Japan,[99] so I do not have confidence that operating honeypots is a valuable method of investigation.

---

[97] Code of Criminal Procedure (Act No. 131 of 1948).
[98] Act on Communications Interception for Criminal Investigation (Act No. 137 of 1999).
[99] *令和３年中の通信傍受の実施状況等に関する公表 (Announcement of the status of interception of communications during 2021)*. Ministry of Justice, https://www.moj.go.jp/keiji1/keiji11_00016.html; Bert-Jaap Koops and Susan W.

Conclusion

While a comparison of legal systems is not always helpful, since the structure of the U.S. and Japanese legal systems are quite different, it is important to compare the factors and how they are taken into account when considering a particular act to be a crime, regardless of the differences between the legal systems. As I have seen, the difference between "authorized access" and "excess authorization" and the factors to be considered are also helpful in examining the application of the statute in Japan.

Japan's interest in policing cybercrime grew in the 1980s, and originally, Japan was not far behind in comparison to the world's standards. On the other hand, Japan lagged behind the United States by nearly 20 years when it came to criminalizing the "act of unauthorized computer access" itself. It is necessary to acknowledge the delays and learn from the situation in other countries.

The role of the CFAA in the United States may be returning to the form it was in when the law was enacted, thanks to *Van Buren v. United States*. In other words, it will no longer be a means of dispute resolution between retired employees and corporations, but rather will specialize in functioning as a law to protect the important information of U.S. government agencies and financial institutions. The role of the CFAA as a criminal statute will remain significant, while its role as a civil statute will be shrinking.

Brenner, editors. *Cybercrime and Jurisdiction: A Global Survey*. TMC Asser; Cambridge University Press [distributor], 2006: 246.

In Japan, cybercrime will be addressed primarily in Penal Code and APUCA. In particular, the role of APUCA as a criminal law is expected to expand day by day. I should point out, however, that there have been few court decisions concerning cybercrime, especially involving APUCA, which might be attributed to the lack of challenge, a cautious investigation by Japanese authorities, or characteristics of the legal system itself, and this lack of court decisions makes it particularly difficult to improve the legal framework to combat cybercrime in Japan. As a result, it may be necessary to reflect on whether law enforcement agencies are only cracking down on cybercrimes that are easy to deal with.

Both the United States and Japan have created a basic legal framework for dealing with cybercrime at this time and have almost similar statutes and penalties. Cybercrime differs from traditional crimes targeting humans or physical objectives in that computers are used as tools and are also the target of criminal acts. I have confirmed that there is no significant difference between the legal frameworks of the two countries, so what Japanese law enforcement needs to work on in the future will be to improve its practical capabilities. I will also continue to consider what is best for policing cybercrime.

TABLES

Table 1

U.S.C		JP: P.C, APUCA
1030(a)(1)	Cyber Espionage	N/A (Covered Like Other Traditional Crimes and APUCA articles 3,4)
1030(a)(2)	Obtaining Information by Unauthorized Access	N/A (Covered Like Other Traditional Crime and APUCA articles 3,4)
1030(a)(3)	Government Computer Trespassing	APUCA article 3
1030(a)(4)	Computer Fraud	P.C article 246-2
1030(a)(5)	Damaging a Computer: Cyber Attack	P.C article 234-2
1030(a)(6)	Password Trafficking	APUCA article 4
1030(a)(7)	Cyber Threatening and Extortion	N/A (Covered Like Other Traditional Crime and P.C articles 161-2, 168-2, 168-3)

Table 2

	Imprisonment (Maximum)	Fine (Maximum)
U.S.C (CFAA)	20 years (Felony)	$ 250,000
P.C	10 years	￥1,000,000 ($ 7,316)
APUCA	3 years	￥1,000,000 ($ 7,316)

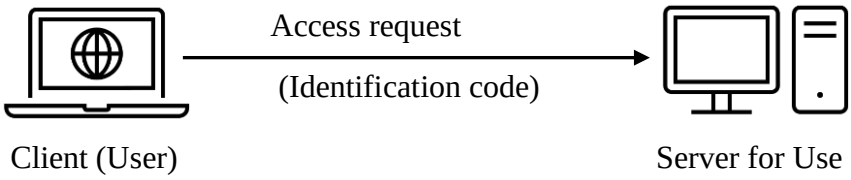
$1.00 = ￥ 136.69 (Central rate of May 1, 2023)

FIGURES

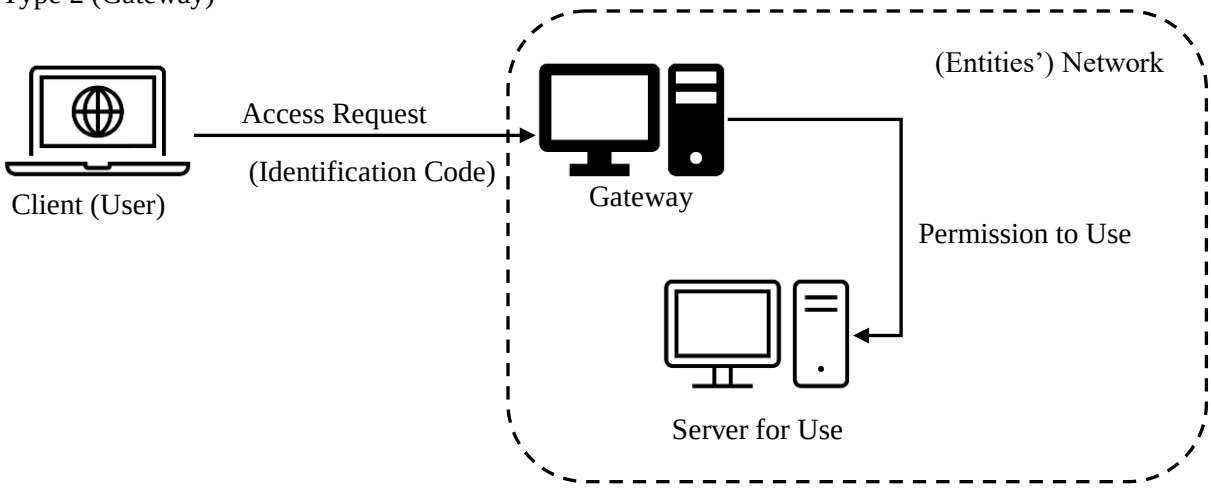
Figure 1

Pattern of Specified Computer With Access Control Feature

Type 1 (Basic)



Type 2 (Gateway)



Type 3 (Authentication Server)

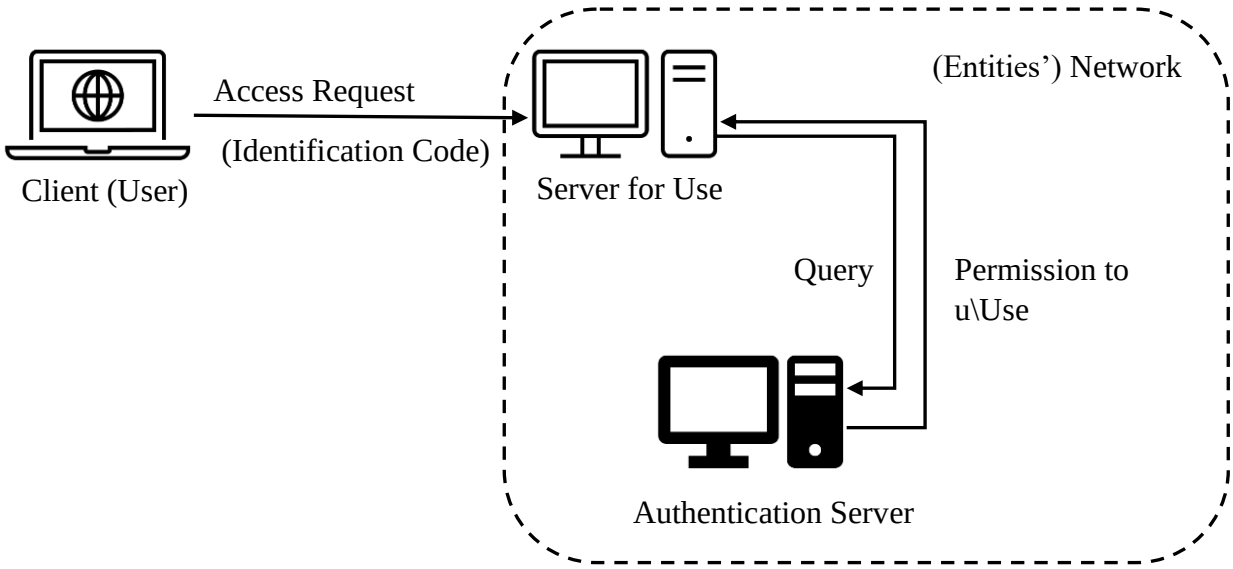
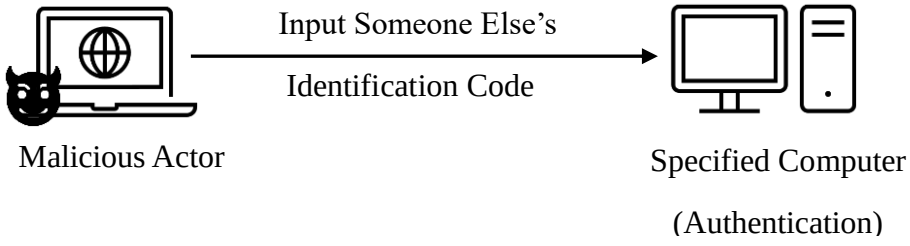


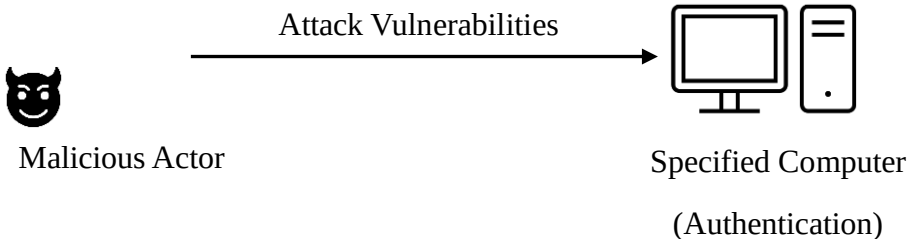
Figure 2

Pattern of Act of Unauthorized Computer Access

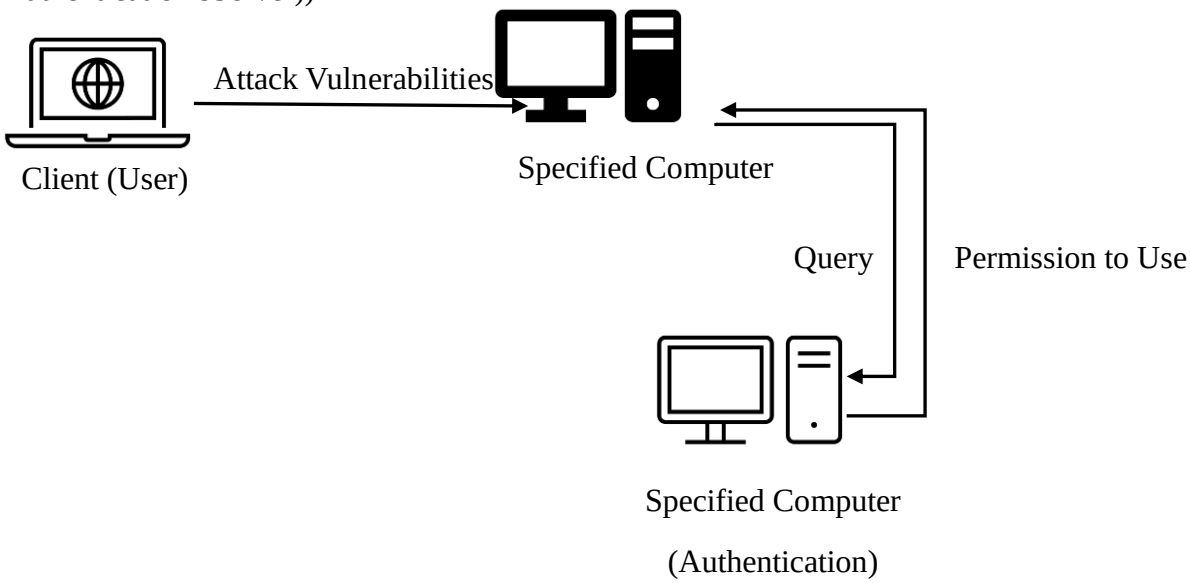
Type 1 (Article 2(4)(i); Unauthorized Log-in)



Type 2 (Article 2(4)(ii); SecurityHole (a: Attacking the Authentication Server Directly))



Type 3 (Article 2(4)(iii); Security Hole (b: Attacking a Computer That Is Not an Authentication sServer))



BIBLIOGRAPHY

"サイバー警察局とは (About the Cyber Affairs Bureau)". NPA, https://www.npa.go.jp/bureau/cyber/what-we-do/about.html. Accessed 24 May 2023.

令和３年中の通信傍受の実施状況等に関する公表 (Announcement of the status of interception of communications during 2021). Ministry of Justice, 2022, https://www.moj.go.jp/keiji1/keiji11_00016.html.

Berris, Peter G. *Ransomware and Federal Law: Cybercrime and Cybersecurity*. Congressional Research Service, 2021, https://crsreports.congress.gov/product/pdf/R/R46932.

Bianucci, Macon, et al. "Computer Crimes." *American Criminal Law Review*, vol. 59, no. 3, Summer 2022, pp. 511-70. *HeinOnline*, https://heinonline-org.ezp-prod1.hul.harvard.edu/HOL/P?h=hein.journals/amcrimlr59&i=527.

Complaint & Demand for Jury Trial at 1, WhatsApp, Inc. & Facebook, Inc. v. NSO Grp. Technologies Ltd. & Q Cyber Technologies Ltd., No. 3: 19-cv-07123, 2015 WL 1033734 (N. D. Cal. Oct. 29, 2019)

Computer fraud legislation : Hearing before the Subcommittee on Criminal Law of the Committee on the Judiciary, United States Senate, Ninety-ninth Congress, first session, on S. 440 .. and S. 1678 .. October 30, 1985. . , . HeinOnline, https://heinonline-org.ezp-prod1.hul.harvard.edu/HOL/P?h=hein.cbhear/cmpfrudle0001&i=1.

The Computer Fraud and Abuse Act of 1986. Hearing before the Committee on the Judiciary, United States Senate, Ninety-Ninth Congress, Second Session on S.2281, a Bill To Amend Title 18, United States Code, To Provide Additional Penalties for Fraud and Related Activities in Connection with Access Devices and Computers, and for Other Purposes. Superintendent of Documents, U, 16 Apr. 1986. *ERIC*, https://eric.ed.gov/?id=ED282520.

"Congressional Record." *Congress.gov*, Library of Congress, 22 May 2023, https://www.congress.gov/congressional-record/volume-166/issue-163/house-section/article/H4581-1.

Clough, Jonathan. *Principles of Cybercrime*. Cambridge University Press. 2010

Chase-Sosnoff, Emily, and Shane T. Muñoz. "Understanding the Bounds of the Computer Fraud and Abuse Act in the Wake of Van Buren." *Florida Bar Journal*, vol. 96, no. 2, Apr. 2022, pp. 22–29.

"犯罪統計 (Crime Statistics)", NPA, https://www.npa.go.jp/publications/statistics/sousa/statistics.html. Accessed 24 May 2023.

Cunningham, McKay. *Cyber Law in the United States of America*. Kluwer Law International B.V, 2020.

"国民のためのサイバーセキュリティサイト (Cybersecurity website for nationals)", Ministry of Internal Affairs and Communications, https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/basic/basic_legal_02.html. Accessed 24 May 2023.

Doyle, Charles. *Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws*. Federation of American Scientists, 15 Oct. 2014. *ProQuest*, https://www.proquest.com/docview/1820784447?parentSessionId=hGPY10D5yiPhH6usQKYxo2knlfvsJNcV2oVrF1AYxXg%3D&pq-origsite=primo&.

Gramlich, John. "Only 2 percent of Federal Criminal Defendants Go to Trial, and Most Who Do Are Found Guilty." *Pew Research Center*, https://www.pewresearch.org/short-reads/2019/06/11/only-2-of-federal-criminal-defendants-go-to-trial-and-most-who-do-are-found-guilty/.

Griffith, Dodd S. "The Computer Fraud and Abuse Act of 1986: A Measured Response to a Growing Problem" *Vanderbilt Law Review*, vol. 43, no.2, 1990, pp. 453-90

Husei Akusesu Taisaku Housei Kenkyukai. *逐条 不正アクセス行為の禁止等に関する法律［第二版］ (Article-by-article Explanation: The Act on the Prohibition of Unauthorized Computer Access 'Second edition')*. Tachibana shobo, 2012.

"H.R.3270 - 116th Congress (2019-2020): Active Cyber Defense Certainty Act." *Congress.gov*, Library of Congress, 28 June 2019, https://www.congress.gov/bill/116th-congress/house-bill/3270.

Internet Crime Complaint Center. *Internet Crime Report 2021*. FBI, Mar. 2022, www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf.

Jarrett, H. Marshall, et al. *Prosecuting Computer Crimes*. Office of Legal Education Executive Office for United States Attorneys, 2010, www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf.

Kerr, Orin S. *Computer Crime Law*. Fourth edition, St. Paul, MN: West Academic Publishing, 2018.

---., 'Cybercrime's Scope: Interpreting Access and Authorization in Computer Misuse Statutes', *New York University Law Review*, 78.5 (2003), 1596–1668

---.. “Vagueness Challenges to the Computer Fraud and Abuse Act” *Minnesota Law Review*, vol.94, no.5, May 2010, pp.1561-87.

---. “Focusing the CFAA in Van Buren” *The Supreme Court Review*, vol. 2021, 2021, pp.155–84.

Koops, Bert-Jaap, and Susan W. Brenner, editors. *Cybercrime and Jurisdiction: A Global Survey*. TMC Asser ; Cambridge University Press [distributor], 2006.

Office of the Deputy Attorney General. *Report of the Attorney General’s Cyber Digital Task Force*. DOJ, July 2018, www.justice.gov/archives/ag/page/file/1076696/download.

Office of the Federal Register, National Archives and Records Administration. 98 Stat. 1837 - Acquisition of Foreign Evidence Improvements Act. U.S. Government Publishing Office: 98 Stat. 2190, https://www.govinfo.gov/app/details/STATUTE-98/STATUTE-98-Pg1837.

---. 108 Stat. 1796 - Anti-Corruption Act of 1993. U.S. Government Printing Office: 108 Stat. 2097, https://www.govinfo.gov/app/details/STATUTE-108/STATUTE-108-Pg1796.

---. 110 Stat. 3488 - National Information Infrastructure Protection Act of 1996. U.S. Government Printing Office: 110 Stat. 3488, 3491, https://www.govinfo.gov/app/details/STATUTE-110/STATUTE-110-Pg3488.

---. Public Law 107 - 56 - Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001. U.S. Government Printing Office, 25 Oct 2001: 115 Stat. 373, https://www.govinfo.gov/app/details/PLAW-107publ56.

---. Public Law 110 - 326 - An act to amend title 18, United States Code, to provide secret service protection to former Vice Presidents, and for other purposes. U.S. Government Printing Office, 25 Sep 2008: 122 Stat. 3561, https://www.govinfo.gov/app/details/PLAW-110publ326.

---. Public Law 116 - 179 - Defending the Integrity of Voting Systems Act. U.S. Government Publishing Office, 19 Oct 2020: 134 Stat. 855, https://www.govinfo.gov/app/details/PLAW-116publ179.

177th Diet Session, House of Representatives, Committee on Judicial Affairs, No. 13, May 25, 2011, Statement of Purpose of the Act for Partial Revision of the Penal Code, etc. to Cope with Advanced Information Processing, etc., https://www.shugiin.go.jp/internet/itdb_kaigirokua.nsf/html/kaigirokua/000417720110525013.htm. Accessed 24 May 2023.

Otsuka, Hitoshi, et al. *大コンメンタール刑法[第三版]第12巻 (Grande Commentaire Criminal Law [3rd ed.], Vol. 12).* Seirin-Shoin, 2019.

Penney, Jonathon W., and Bruce Schneier. “Platforms, Encryption, and the CFAA: The Case of WhatsApp v. NSO Group.” *Berkeley Technology Law Journal*, vol. 36, no. 1, 2021, pp. 469-510.

Podgor, Ellen S. “Counterfeit Access Device and Computer Fraud and Abuse Act of 1984.” *Major Acts of Congress*, edited by Brian K. Landsberg, vol. 1, Macmillan Reference USA, 2004, pp. 194–97. Gale eBooks, *Gale*, https://link.gale.com/apps/doc/CX3407400069/GVRL?sid=bookmark-GVRL&xid=d9e36f93.

Pollaro, Greg. “Disloyal Computer Use and the Computer Fraud and Abuse Act: Narrowing the Scope,” *Duke Law & Technology Review*, vol. 9, 2010-2011, pp. [1]-[11].

Standage, Tom. *The Crooked Timber of Humanity*. The Economist, 5 Oct. 2017, https://www.economist.com/1843/2017/10/05/the-crooked-timber-of-humanity.

令和３年におけるサイバー空間をめぐる脅威の情勢等について (Threats Related to Cyber Space in 2021). NPA, Apr. 2022, www.npa.go.jp/publications/statistics/cybersecurity/data/R03_cyber_jousei.pdf

Tompkins, Joseph B. Jr., and Linda A. Mar. “The 1984 Federal Computer Crime Statute: A Partial Answer to a Pervasive Problem.” *Computer/Law Journal*, vol. 6, no. 3, Winter 1986, pp. 459-84.

Tompkins, Joseph B. Jr., and Frederick S. Ansell. “Computer Crime: Keeping up with High Tech Criminals.” *Criminal Justice*, vol. 1, no. 4, Winter 1987, pp. 31-46.

United States Congress House Committee on the Judiciary Subcommittee on Civil and Constitutional Rights. *Computer Crime: Hearing Before the Subcommittee on Civil and Constitutional Rights of the Committee on the Judiciary, House of Representatives, Ninety-Eighth Congress, First Session ... November 18, 1983*. U.S. Government Printing Office, 1984, https://books.google.com/books?id=G0nRxQEACAAJ.

United States, Supreme Court. *Van Buren v. United States*. 3 June 2021. *Legal Information Institute*, Cornell U Law School, https://www.law.cornell.edu/supremecourt/text/19-783.

令和４年版警察白書 (The White Paper on Police 2022). NPA, 2022, https://www.npa.go.jp/hakusyo/r04/index.html