サイバー犯罪の研究（一）-DoS 攻撃（DDoS 攻撃）に関する比較法的検討-

法律論叢　第八五巻　第一号（二〇一二・七）

【論　説】

サイバー犯罪の研究（一）

――DoS攻撃（DDoS攻撃）に関する比較法的検討――

夏井高人

目　次

一　はじめに

サイバー犯罪（Cybercrimes）とは、①コンピュータシステムを固有の構成要件要素とする犯罪及び②コンピュータシステムを利用して実行される犯罪の総称である。(1) サイバー犯罪と類似の法概念として、コンピュータ犯罪（Computer crimes）、ネットワーク犯罪（Network crimes）、ハイテク犯罪（High-technology crimes）(2) 及び情報犯罪（Information crimes）等がある。

一般に、「サイバー犯罪」と呼ばれる違法行為類型の中には、日本国の刑罰法令によって処罰可能なものとそうでないものとが含まれる。そのため、厳密には、処罰可能でない違法行為について「犯罪」という名称を用いることについて、罪刑法定主義の観点からの異論があり得る。

しかしながら、社会現象としての「サイバー犯罪」を考察するとすれば、日本国の国家主権の物理的範囲に限定して考察することは妥当ではない。なぜなら、「サイバー犯罪」は、①主権国家の国境を越えて実行され得るものであり、②日本国においては日本国の法令によって処罰することができない違法行為であっても、世界のどこかの国において当該国の法令によって処罰されることがあり得るものであり、③それゆえに、当該処罰可能な国の捜査機関から国際的な捜査協力の依頼を受ける可能性のあるものであるからである。かつ、④日本国も加盟し国会の承認を得ている欧州サイバー犯罪条約（Convention on Cybercrime (CETS No.185, Budapest, 23 November 2001)）(3) によって「サイバー

犯罪」が定義されており、その定義に従い、日本国においても条約に定める「サイバー犯罪」を処罰可能とするための法令を立法しなければならない国際的な義務のある違法行為が存在している。(4) 加えて、⑤欧州サイバー犯罪条約についてはEUの関連委員会等において見直し作業が継続的になされており、同条約に定める「サイバー犯罪」の定義によっては処罰不可能な行為類型（例えば、フィッシング等）について検討が重ねられている。このような検討作業は、例えば、日本国においても不正アクセス禁止法の一部改正の議論等に対して直接・間接に影響を与えている。これらのことから、この領域においては、立法論に属する事柄についても「サイバー犯罪」という概念に含めて論議せざるを得ない場合があるという特殊性がある。

本論文は、「サイバー犯罪」に関する既述のような国際的法状況とりわけ立法動向を踏まえ、日本国の法令によっては処罰されない違法行為をも含めて「サイバー犯罪」と呼ばれる一群の違法行為が存在することを認めた上で、そのような違法行為に対して適用可能な日本国刑罰法令とその法解釈、海外における関連法令との比較法的検討及び立法論等を、主要な違法行為の類型に着目して調査・検討した結果を論述し、それによって今後の刑事司法における理論研究及び実務に資することを目的とする。

本稿においては、二〇一一年以降現在に至るまで、世界規模で深刻な問題となっている「政府機関や重要産業等を標的とするサイバー攻撃（Cyberattack）」において主要な攻撃手法の一つとして用いられてきたDoS攻撃及びDDoS攻撃を中心として論述する。(5)

二　情報セキュリティの領域における DoS 攻撃（DDoS 攻撃）の定義・概念

一般に、情報セキュリティの領域では、DDoS 攻撃（Distributed Denial of Service Attack）とは、「攻撃者が第三者の多数のサーバに攻撃用プログラムをしかけ、そのサーバ群から標的とするサーバへ大量のパケットを同時に送り込み、サービス不能に陥れる攻撃をいう」[6]等と定義されている。そして、DDoS 攻撃の手法については、「DDoS 攻撃を行うには、攻撃者は多数（攻撃の種類によっては数百～数千台）の侵害されたホストを必要とし、それらのホストが攻撃対象のサーバを過負荷状態にしてクラッシュさせます。侵害されたホストコンピュータは、ゾンビ（Zombie）とも呼ばれます（ゾンビとは、オーナーの知らないうちにデーモンまたはシステムエージェントに感染し、攻撃者によって制御されるコンピュータです）。ホストは自動化ツールを使って侵害され、侵害されるとマスターホストによる制御が可能になります。マスターホストは、すべてのゾンビホストから攻撃対象サーバへの同時攻撃を調整します」とされている。[7]

その語源からすれば、DDoS 攻撃という用語は、DoS 攻撃（Denial of Service Attack）から派生したものとされている。例えば、DoS 攻撃とは、一般に、「サーバを標的とし、それを利用不可能な状態とすることを狙った大量のトラフィックの送信を実行するサイバー攻撃の一種」として理解されている。[8] DoS 攻撃のために用いられるコンピュータ装置等は複数であることを要しない。例えば、後述の David Lennon 事件のような電子メール爆弾攻撃では、一個のＰＣから攻撃を実行することが可能であり、標的となるサーバの処理能力が十分でない場合には一個のＰＣから送信される大量の攻撃パケットだけで当該サーバをダウンさせることが可能である。

要するに、DDoS 攻撃とは、DoS 攻撃の中でも多数の攻撃用マシンまたはゾンビマシン[9]から協調的または同時的になされる集中攻撃的ないし飽和攻撃的なタイプのものを特に指すものとして理解することができる。DDoS 攻撃では、複数の攻撃用マシンまたはゾンビマシンから攻撃パケットが送出されるため、DoS 攻撃において一個のＰＣから送出される攻撃パケットよりもはるかに大量の攻撃パケットを送出することが可能である。その結果、十分な処理能力を有するタフなサーバでも DDoS 攻撃によって誤作動[10]を生じたりダウンしたりすることがある。

一般に、DDoS 攻撃は、一九九〇年代から顕著に検出されるようになったものとされている。例えば、一九九八年には米国連邦の海軍や空軍等のサーバが、サンマイクロシステムズ社の Solaris を標的とするように予めセットされた DDoS 攻撃を受けた[11]。また、一九九九年五月には米国ＦＢＩのウエブサイトが、DDoS 攻撃を受け、二〇〇〇年二月には Yahoo, eBay, Amazon などの著名企業のウエブサイトが攻撃を受けた[12]。二〇一一年以降には「アノニマス（Anonymous）」を名乗るグループ[13]が世界各国の政府（官庁、軍、警察、裁判所など）や著名企業（特に金融・証券業、軍事産業、インフラ関連産業等）に対して苛烈な攻撃を加え続け、多数のウエブサイトが運用不能となったり（破壊）、サービス提供の継続が不可能となってシャットダウンに追い込まれたりするような事態が発生している[14]。

このように深刻な被害を発生させてきた DDoS 攻撃における攻撃手法は、その被害が物体であるサーバに生ずるとしても、攻撃それ自体としてはあくまでも電子的なものであり、いわゆるボットネットなどを通じて多数のゾンビマシンから同時的に攻撃パケットを送出することによって実行されるものではある。しかし、その基本は、物理的な武器（対艦ミサイル等）を用いた軍事攻撃としての飽和攻撃と論理的には同種のものに属すると考えることができる。DDoS 攻撃を受けたサーバは、大量に送信されてくる攻撃パケットに対する対応や処理が不可能となり、飽和状態となって誤作動を生じさせたり、その機能を停止させたりすることになる。このようなことは、意図的な攻撃ではない

単なるアクセスの集中によっても偶発的に生ずることがあり得る。しかし、そのような不具合や障害が意図的なトラフィックの集中送信によって実行されるところに故意行為としてのDDoS攻撃の本質がある。換言すると、DDoS攻撃は、いわば「標的となるサーバ等に対する電子的な飽和攻撃である」と表現することができる。(15)

他方、DDoS攻撃を実行するためには、攻撃用のプログラムが必要となる。そのプログラムは、攻撃者自身が作成するのが普通であったため、かなり高度な能力を有する者でなければ攻撃者となることができないと考えられてきた。しかし、今日、ソーシャルメディアなどを利用して攻撃者（攻撃者予備軍）が情報交換を行うことができるようになっているため、(16)誰かが最初に攻撃用プログラムを作成すると、その作成のための情報が比較的容易に攻撃者（攻撃者予備軍）に伝播するという現象がみられる。また、攻撃用プログラムがツール化され、有償・無償で流通し、全くの素人でも容易に攻撃者となることができるというような事態も生じている。(17)これらのことから、今後、高度な技術や能力を有する者に限定されず、かなり広範なタイプの者が加害者となって、DDoS攻撃が更に多数発生する可能性があることを否定することができない。

三　法律用語としてのDoSの定義・概念（米国州法）

このDoS（Denial of Service）は、米国の法律用語（英語）として古くから存在しているし、この用語を用いた立法例（米国各州の刑法等）が多数存在する。おそらく、法律用語としての「DoS」が一般用語化し、更に情報セキュリティの分野に転用されて今日に至っているものと推測される。

DoS（Denial of Service）は、直訳すれば「サービス拒否」となる。(18)しかし、法律用語としては、特定のコンピュー

タサービスの提供者がサービスの提供を拒否することを意味するのではなく、特定のコンピュータサービスの提供者の業務遂行を妨げることによって、その利用者がサービスの提供を受けることができない状態にすることを意味している。換言すると、サービス提供が拒否されるような状態にすることを意味している。

例えば、米国フロリダ州の犯罪法（Title XLVI）の Chapter 815.06(1)(b)[19] は、コンピュータ利用者に対する犯罪（Offenses against computer users）を実行する行為について、次のとおりに規定している。

八一五・〇六　コンピュータ利用者に対する犯罪

(1)　意図的に、認識して、かつ、無権限で

(b)　その全部もしくは一部について、他人によって保有され、他人との契約関係の下にあり、他人のために管理され、他人のためのものであり、もしくは、他人と共有関係にあるようなコンピュータシステムの利用に関する権限を有する利用者に対するコンピュータシステムの利用を混乱させた者、拒否した者、または、拒否を発生させた者

は、コンピュータ利用者に対する犯罪を実行する者である。

815.06 Offenses against computer users

(1) Whoever willfully, knowingly, and without authorization:

(b) Disrupts or denies or causes the denial of computer system services to an authorized user of such computer system services, which, in whole or part, is owned by, under contract to, or operated for, on behalf of, or in

conjunction with another
commits an offense against computer users.

また、例えば、米国カリフォルニア州の刑法典 502.(c)(5) は、コンピュータサービスの提供を拒否する行為について、次のように規定している。(20)

五〇二(c)(5)

認識して、無許可で、コンピュータサービスを混乱させ、もしくは、混乱を発生させた者、または、コンピュータ、コンピュータシステムもしくはコンピュータネットワークの権限を有するユーザに対するコンピュータサービスの提供を拒否し、もしくは、その拒否を発生させた者

502.(c)(5)

Knowingly and without permission disrupts or causes the disruption of computer services or denies or causes the denial of computer services to an authorized user of a computer, computer system, or computer network.

加えて、例えば、米国ネバダ州の犯罪及び刑罰法典 NRS 205.477 は、コンピュータシステム等へのアクセス妨害行為について、次のように規定している。

二〇五・四七七

一　第三項及び第四項に規定する場合を除き、認識して、意図して、かつ、無権限で、コンピュータ、システムもしくはネットワークを使用する権利及び義務を有する者に対し、その使用またはアクセスを妨害し、それらを拒否し、または、それらを拒否されるようにした者は、軽罪として有罪である。

NRS 205.477 Unlawful interference with or denial of access to or use of computers; unlawful use or access of computers; affirmative defense.

1. Except as otherwise provided in subsections 3 and 4, a person who knowingly, willfully and without authorization interferes with, denies or causes the denial of access to or use of a computer, system or network to a person who has the duty and right to use it is guilty of a misdemeanor.

類似の立法例は、米国の多数の州法（刑法等）の中に存在する。

要するに、米国の犯罪法におけるDoSとは、無権限で、適法な利用者がコンピュータサービスの利用の提供を受けることができない状態にすることを意味している。これらの米国州法におけるDoSに関する条項は、日本国の刑法における電子計算機損壊等業務妨害罪（刑法二三四条の二）と同趣旨のものとして理解することができる。

そして、情報セキュリティの分野においても違法な行為とされているDoS攻撃を処罰可能な行為として理解しなければならない場合には、法概念との整合性を保つため、上記のフロリダ州法の例にみられるように、コンピュータサービスの利用者が、当該コンピュータサービスの提供を受けられないような状態にする行為のことをDoSと理解し、ま

た、DoSの実行のために第三者の多数のコンピュータがゾンビマシンとして利用され、同時的に攻撃が実行される場合をDDoSとして理解するのが妥当である。

以下、本稿においては、上記のような意味でDDoS攻撃という語を用いることにする。

四　適用可能な日本国刑罰法令

1　ゾンビマシンを構成するための攻撃に適用可能な刑罰法令

DoS攻撃は、必ずしもゾンビマシンを必要とせず、攻撃者が保有するマシンから直接に攻撃をしかけることが（理論上では）可能である。(21)

これに対し、DDoS攻撃では、大量の攻撃パケットを同時かつ集中的に送信するために、多数のゾンビマシンが必要である。その意味で、DDoS攻撃では、攻撃者が保有するマシンではなく第三者が保有する多数のマシンの存在が必須となる。

第三者が保有するマシンをゾンビマシンとしてしまう手法（技術）には様々な態様のものがあり得る。例えば、DDoS攻撃を実行するためのボットネットを構築するためのボットプログラムその他のマルウェアを、第三者宛の電子メールに添付したり、第三者がダウンロードしたコンテンツに予め組み込んでおいたり、偽セキュリティサイトなどから予めマルウェアを組み込んだ偽のセキュリティソフトをダウンロードさせたり（スケアウェア）(22)、無害なサイトから無害なコンテンツ（アプリケーション）をダウンロードする際にマルウェアも一緒にダウンロードするようにしたり（ダ

ウンロードバイアプリケーション）するような手法が現実に存在する。

そして、第三者のマシンの管理を奪い、それを支配することができるようなマルウェアは、ボットネットを通じて遠隔操作され、あるいは、論理爆弾（logic bomb）の手法と同様にタイマーによって自律的に、特定の日付・時刻になると一斉に攻撃用パケットを送信し始めることになる。

これらの行為は、DDoS 攻撃の実行行為の前になされる準備的行為（予備行為）として理解することが可能であるが、立法論としては、この準備的行為それ自体としても犯罪を構成するものとすることが考えられる。

第三者のマシンをゾンビマシン化するための手法は実に多種多様であり、それぞれの行為に即して犯罪の成否を考えなければならない。ただし、ボットネットなどを介して第三者の管理を排除し支配を奪う行為は、その第三者のマシンにアクセス制御がなされているときは、不正アクセス罪を構成するものと解される。

また、第三者のマシンが当該第三者の事務処理のために供されている場合には、当該第三者のマシンについて後述の電子計算機損壊等業務妨害罪が成立することがあり得る。

他方、第三者のマシン内に既にインストールされている正常なソフトウェアの一部を改変し、DDoS 攻撃を実行するためのマルウェアとして機能するように変化させてしまう行為は、改変されたソフトウェアが著作物であるときは、著作権法違反（同一性保持権の侵害）の罪を構成することがあり得ると解される。(23)

そして、DDoS 攻撃を実行するために、第三者の保有するゾンビマシン内にインストールされたマルウェアを起動・実行させるためには、少なくとも一アンペア以上の電力を消費することが明らかであるから、事案によっては、電気窃盗罪（刑法二四五条）の成立を検討すべき場合もあるのではないかと思われる。

2　実行されたDDoS攻撃に適用可能な刑罰法令

(1)　電子計算機損壊等業務妨害罪

DoS攻撃については、電子計算機損壊等業務妨害罪（刑法二三四条の二第一項）が成立し得ると解するのが通説である。[24] DDoS攻撃については、従来、特に詳しく論じられたことはないと思われるが、DDoS攻撃がDoS攻撃の一つの類型であることからすれば、DoS攻撃と同様、電子計算機損壊等業務妨害罪（刑法二三四条の二第一項）と解するべきである。

電子計算機損壊等業務妨害罪（既遂罪）の実行行為は、①電子計算機もしくはその用に供する電磁的記録を損壊すること、②虚偽の情報もしくは不正な指令を与えること、または、③その他の方法のいずれかである。DDoS攻撃では、一般に、攻撃用パケットが大量に集中的・同時的に送信されることによって実行されるものであるが、そのパケットの内容の相違に従い、②虚偽の情報もしくは不正な指令を与える場合、または、③その他の方法に該当するものと解される。

一般に、「不正な指令」とは、コンピュータに対して入力される命令のことを指すが、命令それ自体が不正である場合（当該コンピュータによって処理することが不能である場合）には絶対に既遂に達することがあり得ないので不能犯となる。[25] したがって、ここにいう「不正」とは、命令それ自体として不正であるという意味ではなく、「権限なく、当該コンピュータによって処理可能な命令が与えられる」ということを意味すると解するほかはない。そして、攻撃対象により処理可能な命令が大量に送信された場合、不正な指令を与えることによる電子計算機損壊等業務妨害罪の

成立を検討すべきことになる。例えば、第三者のログオン用ＩＤを大量かつ集中的・同時的に入力するというDDoS攻撃が実行された結果、攻撃対象であるコンピュータシステム上で同一のＩＤ保有者による重複したアクセスを排除するための処理が過負荷となり、当該コンピュータシステムのアクセス制御処理が適正に実行できない状態を発生させた場合などを考えることができる。(26)

一般に、DDoS攻撃で用いられる攻撃用パケットには、全く意味のないデータで構成されているものがある。この場合、全く意味のないデータである以上、「虚偽」もあり得ないので「虚偽の情報」とは言えないし、また、「不正な指令」と言うこともできない。このような全く意味のないデータによる攻撃の場合には、「その他の方法」に該当するものと解するべきであろう。

(2) **器物損壊罪**

DDoS攻撃の結果、攻撃を受けたコンピュータシステムに物理的な損傷が発生した場合（ハードディスクのクラッシュ、スイッチ類の破損、通信ケーブルの焼損など）は、器物損壊罪（刑法二六一条）が成立する。(27)

電子計算機損壊等業務妨害罪（刑法二三四条の二第一項）と器物損壊罪が成立する場合の罪数については、観念的競合と解するのが通説である。(28)

3 未遂行為、予備行為、準備行為に適用可能な刑罰法令

従来、電子計算機損壊等業務妨害罪（刑法二三四条の二）には未遂行為を処罰する条項が存在しなかった。また、同条の二には準備罪及び予備罪の条項も存在しなかったので、電子計算機損壊等業務妨害罪の準備罪または予備罪とし

ての処罰もなかった。

そのため、裁判所は、未遂行為または準備的行為と評価すべき行為まで業務妨害行為の既遂行為として評価して処罰する傾向が強かった。一般に、このような裁判所の解釈態度が業務妨害罪の本質に関する刑法学上の議論に大きな悪影響を及ぼしていたことは否定できない。

そのような刑法学上の議論の中で、裁判所の傾向について肯定的な傾向を有する論者の多くは、裁判所が業務妨害罪の罪質について抽象的危険犯説を採用していると理解することが多かったように思われる。しかし、正確ではない。裁判所は、罪刑法定主義を軽視し、本来であれば未遂行為または準備的行為（予備行為）として無罪とすべき行為まで「既遂」として処罰してきたのだと理解するのが正しい。

このような理論上及び実務上の問題は、平成二三年六月二四日法律第七四号による刑法等一部改正により、電子計算機損壊等業務妨害罪の規定（刑法二三四条の二）が改正され、従来からある既遂罪は同条の二第一項となり、これに加えて未遂処罰条項が同条の二第二項として追加規定されるに至った。

この一部改正の結果、電子計算機損壊等業務妨害罪については抽象的危険の発生だけで既遂となると解するとすれば未遂罪（刑法二三四条の二第二項）が適用されることがほぼ完全になくなってしまうことになると考えられることから、裁判所は、同条の解釈・運用を変更しなければならない客観的な状態に置かれていると理解することができる。すなわち、刑法一部改正後の電子計算機損壊等業務妨害罪については、論理的には、具体的危険犯として解する以外になく、抽象的危険犯として解する余地はないものと考える。

そして、具体的危険が発生した場合には既遂罪となるが、実行行為の着手があっても具体的危険が発生するに至らなかった場合には未遂罪となると解することになろう。

なお、実行行為の着手のない準備行為や予備行為については、別途不正指令電磁的記録作成罪（刑法一六条の二）等が成立する場合を除き、現行法上処罰されない。また、実行行為があっても何らの危険も発生させる可能性のない行為（例えば、誰がどのように使っても全く何も作動・機能しないバグだらけのプログラムを用いて攻撃しようとしたが、やはり何の結果も生じなかった場合など）については不能犯となると解すべきであり、当然のことながら未遂罪も成立しない。

五　ドイツの立法例

ドイツ刑法三〇三条b（StGB § 303b）は、日本国の電子計算機損壊等業務妨害罪の実行行為と同様の行為につき、次のように規定している[29]。ここでは、未遂行為だけではなく予備行為も処罰対象行為として規定されている。

三〇三条b　コンピュータ妨害罪

(1)　他の者にとって本質的に重要なデータ処理を、以下のいずれかによって著しく妨害した者は、三年以下の自由刑または罰金刑に処する。

1．第三〇三条a第一項による行為[30]

2．他の者を加害する目的で、データ（二〇二条a第二項[31]）を入力若しくは送信する行為、又は

3．データ処理システム若しくはデータ記録媒体を破壊し、損壊し、使用不能にし、消去し若しくは改変する行為

(2) データ処理の遂行が他の者の業務、企業又は官庁にとって本質的に重要である場合、五年以下の自由刑又は罰金に処する。

(3) この罪の未遂犯は、これを罰する。

(4) 第二項において特に重大な場合については、六月以上一〇年以下の自由刑に処する。特に重大な場合とは、次のような場合である。

1. 財産上の重大な損失を発生させる場合
2. 営利目的で実行される場合若しくは継続的にコンピュータ妨害罪を実行する犯罪組織の一員として実行される場合、又は
3. その行為によって、ドイツ連邦共和国の国民に対する重要な物資若しくは役務の供給若しくは国防を危険に晒す場合

(5) 第一項の罪を実行するための予備行為については、二〇二条 c を準用する。

§ 303b Computersabotage

(1) Wer eine Datenverarbeitung, die für einen anderen von wesentlicher Bedeutung ist, dadurch erheblich stört, dass er

1. eine Tat nach § 303a Abs. 1 begeht,
2. Daten (§ 202a Abs. 2) in der Absicht, einem anderen Nachteil zuzufügen, eingibt oder übermittelt oder
3. eine Datenverarbeitungsanlage oder einen Datenträger zerstört, beschädigt, unbrauchbar macht, beseitigt oder

verändert,

wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Handelt es sich um eine Datenverarbeitung, die für einen fremden Betrieb, ein fremdes Unternehmen oder eine Behörde von wesentlicher Bedeutung ist, ist die Strafe Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe.

(3) Der Versuch ist strafbar.

(4) In besonders schweren Fällen des Absatzes 2 ist die Strafe Freiheitsstrafe von sechs Monaten bis zu zehn Jahren. Ein besonders schwerer Fall liegt in der Regel vor, wenn der Täter

1. einen Vermögensverlust großen Ausmaßes herbeiführt,
2. gewerbsmäßig oder als Mitglied einer Bande handelt, die sich zur fortgesetzten Begehung von Computersabotage verbunden hat,
3. durch die Tat die Versorgung der Bevölkerung mit lebenswichtigen Gütern oder Dienstleistungen oder die Sicherheit der Bundesrepublik Deutschland beeinträchtigt.

(5) Für die Vorbereitung einer Straftat nach Absatz 1 gilt § 202c entsprechend.

加えて、ドイツ刑法三一七条（StGB § 317）は、次のように規定している。[32] ドイツにおいては、この三一七条によってDDoS攻撃が処罰可能となる場合があると解される。のみならず、同条は、通信設備に対する妨害行為の未遂犯と過失犯をも処罰するものとしている。

三一七条　通信設備に対する妨害罪

(1)　経営に役立つ物を破壊し、損壊し、除去し、若しくは使用不能にし、又は経営のために予定されている電力を奪うことによって、公共の目的に役立つ遠距離通信設備の操業を阻止し、又は危険にした者は、五年以下の自由刑又は罰金に処する。

(2)　この罪の未遂犯は、これを罰する。

(3)　過失によってこの行為を行った者は、一年以下の自由刑又は罰金に処する。

§ 317 Störung von Telekommunikationsanlagen

(1) Wer den Betrieb einer öffentlichen Zwecken dienenden Telekommunikationsanlage dadurch verhindert oder gefährdet, daßer eine dem Betrieb dienende Sache zerstört, beschädigt, beseitigt, verändert oder unbrauchbar macht oder die für den Betrieb bestimmte elektrische Kraft entzieht, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) Der Versuch ist strafbar.

(3) Wer die Tat fahrlässig begeht, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

これらの条項は、DDoS 攻撃のようなタイプのサイバー犯罪に対する法的対応を検討する際に非常に有益なものであるし、また、日本国における今後の立法においても参考になるものと思われる。

無論、過失犯まで処罰すべきかどうかについては議論が分かれ得ると思われる。しかし、例えば、スマートフォン用

のアプリケーションプログラム（いわゆる「アプリ」）を作成・提供する企業が、製品であるアプリを提供する前の時点で、十分な検査・点検をせず、DDoS攻撃その他の有害な結果を生じさせるコンピュータウイルス（マルウェア）が当該アプリに混入してしまっていることに気づかずそのまま出荷してしまったというような事例(33)を考えてみると、過失犯処罰についても検討すべき余地が十分にあり得るのではないかと考える。

六　有罪の事例

日本国においては、DDoS攻撃を実行したという犯罪事実により有罪判決がなされた事例はない。海外においては、逮捕例が多数あるが、有罪判決となる前に釈放されている例もあり、正確な有罪判決数をつかみにくい状況にある。

一般に、海外の裁判所による有罪判決の事例であっても、日本の司法における量刑判断等に有益な情報の一種と考えられる。それゆえ、今後、この分野での事例の集積・研究がもっと活発になされるべき必要性があるのではないかと考える。

本稿では、比較的有名な事例をいくつか紹介するのにとどめる。

1　スペインの事例：Santiago Garrido 事件

二〇〇六年二月、Santiago Garrido という男（二六歳）に対し、スペインにあるラ・コルーニャ（La Coruña）の裁

判所は、拘禁刑二年の判決を宣告した（ほかに百三〇万ユーロの損害賠償金の支払を命ずる民事判決も言渡し）。

Santiago Garrido は、インターネット上にある『IRC-Hispano』というスペイン語のチャットルームにおいて、規則違反行為があったとして、同チャットルームから追放されアクセス禁止とされたことに立腹し、非常に多数のスペイン人利用者のＰＣにワームを感染させた。このワームは、DDoS 攻撃を実行するためのものであり、標的とされた Wanadoo, ONO, Lleida Net 等のインターネット上のサーバに対し、ワームが感染したＰＣから DDoS 攻撃用の攻撃パケットが集中砲火的に大量送信された。この Santiago Garrido の DDoS 攻撃行為によって被害を受けたのは、スペイン人のインターネット利用者の約三分の一に相当すると推定されている。(34)

なお、スペイン刑法二六四条（判決当時有効な条文）は、次のように規定していた。DDoS 攻撃については、同条二項が適用可能である。

第二六四条

一　以下に示す要件に該当する場合、前条に示す損害を発生させた者は、一年以上三年以下の拘禁刑及び一二月分以上二四月分以下の罰金刑に処す。

1　行政機関の自由な職務行使を妨げるため、もしくは、行政機関の決定に報復するために損害を与え、公務員に対して罪を犯し、証人等として法令や一般法規の執行・適用に寄与する者もしくは寄与できる者に対して罪を犯すこと

2　様々な手段で家畜に感染症もしくは伝染病を起こさせること

3　毒性もしくは腐敗性のある物質を使用すること

4　公共団体もしくは共同体が保有もしくは使用する財産に悪影響を及ぼすこと

5　被害者を破産させ、もしくは、経済的に逼迫した状態に置くこと

二　何らかの方法によって、ネットワーク・システムもしくは情報システムに含まれる他人の電子データ、プログラムもしくは文書を破壊した者、改変した者、使用不能にした者、または、その他の毀損行為をした者は、同様の刑に処す。

Artículo 264.

1. Será castigado con la pena de prisión de uno a tres años y multa de doce a veinticuatro meses el que causare daños expresados en el artículo anterior, si concurriera alguno de los supuestos siguientes:

1. Que se realicen para impedir el libre ejercicio de la autoridad o en venganza de sus determinaciones, bien se cometiere el delito contra funcionarios públicos, bien contra particulares que, como testigos o de cualquier otra manera, hayan contribuido o pueden contribuir a la ejecución o aplicación de las Leyes o disposiciones generales.

2. Que se cause por cualquier medio infección o contagio de ganado.

3. Que se empleen sustancias venenosas o corrosivas.

4. Que afecten a bienes de dominio o uso público o comunal.

5. Que arruinen al perjudicado o se le coloque en grave situación económica.

2. La misma pena se impondrá al que por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informaticos.

2　英国の事例：David Lennon 事件(35)

二〇〇六年五月一一日、英国高等法院は、David Lennon という男（一九歳）の控訴を斥け、DoS 攻撃の実行が英国のコンピュータ濫用禁止法（Computer Misuse Act 1990）違反の罪に該当するとして拘禁刑二月の判決を宣告した。

David Lennon（事件当時一六歳）は、二〇〇三年一二月まで Domestic & General Group PLC（D&G）で労働者として働いていたが、同所を解雇された後、二〇〇四年一月にインターネット上のサイトから電子メール爆弾プログラム Avalanche v3.6 をダウンロードし、これを用いてD&Gを攻撃した。このメール爆弾プログラムは、電子メールサーバに対してサーバの処理能力をはるかに超えた大量の電子メールを送信することにより、そのサーバに障害を発生させ、その結果、そのサーバの電子メール送受信機能を著しく低下させ、または処理不能状態に陥らせることができる。David Lennon は、このプログラムを用いて約五〇〇万通の電子メールを集中送信する攻撃をしかけた結果、D&Gの電子メールサーバ及び同社のウエブサーバ共にダウンしてしまった。しかし、攻撃に用いられたＩＰアドレスをたどる捜査がなされた結果、David Lennon は逮捕され、英国のコンピュータ濫用禁止法違反の罪で起訴された。

第一審の裁判所が有罪としたため控訴がなされたものの、控訴審でも有罪となった。

なお、英国のコンピュータ濫用禁止法（Computer Misuse Act 1990）の第三条は、判決当時、次のように規定されていた。高等法院の判決では、無権限によるコンピュータマテリアルの改変（修正）行為とは、物理的な損壊ではなく使用不能または機能不全状態を発生することを意味するものと解釈すべきかどうかが判示されている。

第三条

(1) 以下の行為を実行した者は、有罪とする。

(a) コンピュータのコンテンツを無権限で修正させる一切の行為を行った者で、

(b) 行為時において、「必要な意図」及び「必要な認識」を有していた者。

(2) 本条第(1)項(b)においては、要件としての「必要な意図」とは、コンピュータのコンテンツに改変を生じさせ、そして、このような行為を実行することによって、

(a) コンピュータの運用を妨害する意図、または

(b) コンピュータ内にあるプログラムもしくはデータにアクセスすることを妨害し、または、これを阻害する意図、または、

(c) 当該プログラムの運用もしくは当該データの信頼性を阻害する意図

のいずれかを意味する。

(3) この「意図」は、以下のいずれかに向けられたものであることを要しない。

(a) 特定のコンピュータ、

(b) 特定のプログラムもしくはデータ、特定の種類のプログラムもしくはデータ、または

(c) 特定の改変もしくは特定の種類の改変

(4) 本条第(1)項(b)においては、要件としての「必要な認識」とは、当該行為者が生じさせようとした改変が無権限のものであるということについての認識をいう。

(5) 本条において、本条第(2)項に示す種類の無権限改変もしくはその意図された効果が、恒久的なものであるか、

一時的なものであるか（もしくは、恒久的なものであることが意図されたか、一時的なものであることが意図されたか）は、重要ではない。

(6)　一九七一年犯罪的毀損行為法（一九七一年一般法律第四八号）においては、コンピュータのコンテンツの改変は、コンピュータまたはコンピュータの記憶媒体に対する毀損行為とみなされてはならない。ただし、コンピュータまたはコンピュータの記憶媒体に与える影響が、物理的な状態を害する場合はこの限りでない。

(7)　本条に基づき犯罪を実行した者として有罪となる者は、次の責任を有する。

(a)　略式裁判が行われる場合、六月以下の拘禁刑もしくは法定の最高額を超えない金額の罰金刑に処し、または、これらを併科する。または

(b)　正式裁判が行われる場合、五年以内の拘禁刑もしくは罰金刑、または、これらを併科する。

3.

(1) A person is guilty of an offence if

(a) he does any act which causes an unauthorised modification of the contents of any computer; and

(b) at the time when he does the act he has the requisite intent and the requisite knowledge.

(2) For the purposes of subsection (1)(b) above the requisite intent is an intent to cause a modification of the contents of any computer and by so doing?

(a) to impair the operation of any computer;

(b) to prevent or hinder access to any program or data held in any computer; or

(c) to impair the operation of any such program or the reliability of any such data.

(3) The intent need not be directed at?

(a) any particular computer;

(b) any particular program or data or a program or data of any particular kind; or

(c) any particular modification or a modification of any particular kind.

(4) For the purposes of subsection (1)(b) above the requisite knowledge is knowledge that any modification he intends to cause is unauthorised.

(5) It is immaterial for the purposes of this section whether an unauthorised modification or any intended effect of it of a kind mentioned in subsection (2) above is, or is intended to be, permanent or merely temporary.

(6) For the purposes of the [1971 c. 48.] Criminal Damage Act 1971 a modification of the contents of a computer shall not be regarded as damaging any computer or computer storage medium unless its effect on that computer or computer storage medium impairs its physical condition.

(7) A person guilty of an offence under this section shall be liable;

(a) on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both; and

(b) on conviction on indictment, to imprisonment for a term not exceeding five years or to a fine or to both.

その後、同法は改正された。二〇一一年四月現在有効な同法第三条の条文は、次のようになっている。

第三条　コンピュータの運用等を侵害する意図による、または、不注意により阻害する無権限行為

(1)　以下の行為を実行した者は、有罪とする。

(a)　コンピュータと関連する無権限の行為を実行した者であり、

(b)　行為時において、その行為が無権限であることを認識しており、かつ、

(c)　以下の第(2)項または第(3)項に該当する者。

(2)　本条は、当該の者が行為時において以下のとおり意図していた場合に適用する。

(a)　コンピュータの運用を阻害すること、

(b)　コンピュータ内にあるプログラムもしくはデータへのアクセスを阻止もしくは妨害すること、

(c)　当該プログラムの運用もしくは当該データの信頼性を侵害すること、または、

(d)　上記第(a)号ないし第(c)号に規定することを実行可能にすること。

(3)　本条は、上記第(2)項第(a)号ないし第(d)号に規定することを実行することになるかどうかについて当該の者が不注意で気づかなかった場合にも適用する。

(4)　上記第(2)項に規定する意図もしくは上記第(3)項に規定する不注意は、以下であることを要しない。(36)

(a)　特定のコンピュータであること、

(b)　特定のプログラムもしくはデータであること、または、

(c)　特定の種類に属するプログラムもしくはデータであること。

(5)　本条においては、

(a)　ある行為を実行するということは、ある行為が実行されるようにすることを含む。

(b) 「行為」は一連の行為である場合を含む。

(c) 侵害、阻害もしくは妨害は一時的にそのようにする場合を含む。

(6) 本条に基づき犯罪を実行した者として有罪となる者は、次の責任を有する。

(a) イングランド及びウェールズにおいて略式裁判が行われる場合には、一二月以下の拘禁刑もしくは法定の最高額を超えない金額の罰金刑に処し、または、これらを併科する。

(b) スコットランドにおいて略式裁判が行われる場合には、六月以下の拘禁刑もしくは法定の最高額を超えない金額の罰金刑に処し、または、これらを併科する。または、

(c) 正式裁判が行われる場合には、一〇年以下の拘禁刑もしくは法定の最高額を超えない金額の罰金刑に処し、または、これらを併科する。

3 Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer, etc..

(1) A person is guilty of an offence if- .

(a) he does any unauthorised act in relation to a computer; .

(b) at the time when he does the act he knows that it is unauthorised; and .

(c) either subsection (2) or subsection (3) below applies. .

(2) This subsection applies if the person intends by doing the act- .

(a) to impair the operation of any computer; .

(b) to prevent or hinder access to any program or data held in any computer; .

(c) to impair the operation of any such program or the reliability of any such data; or .

(d) to enable any of the things mentioned in paragraphs (a) to (c) above to be done. .

(3) This subsection applies if the person is reckless as to whether the act will do any of the things mentioned in paragraphs (a) to (d) of subsection (2) above. .

(4) The intention referred to in subsection (2) above, or the recklessness referred to in subsection (3) above, need not relate to- .

(a) any particular computer; .

(b) any particular program or data; or .

(c) a program or data of any particular kind. .

(5) In this section- .

(a) a reference to doing an act includes a reference to causing an act to be done; .

(b) "act" includes a series of acts; .

(c) a reference to impairing, preventing or hindering something includes a reference to doing so temporarily. .

(6) A person guilty of an offence under this section shall be liable- .

(a) on summary conviction in England and Wales, to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum or to both; .

(b) on summary conviction in Scotland, to imprisonment for a term not exceeding six months or to a fine not

exceeding the statutory maximum or to both; .

(c) on conviction on indictment, to imprisonment for a term not exceeding ten years or to a fine or to both.

七　DDoS攻撃のために利用されたゾンビマシン保有者の罪責

DDoS攻撃のために攻撃プログラムを仕掛けられたＰＣなどゾンビマシンの保有者は、日本国の刑法学における通常の解釈論に基づいて考察してみると、間接正犯のための道具として機能していることになる。ＰＣを含め、いかなるコンピュータといえども電源がオンになっている状態でなければ何らの処理も実行できないから、ゾンビマシンの保有者は、当該ゾンビマシンであるコンピュータの電源をオンにしただけで、実はDDoS攻撃の攻撃者のために寄与をする行為をしていることになる。

このような間接正犯の道具となっている者について、過失犯処罰の規定が存在する場合には、本人が全く知らない間に利用されている場合であっても過失犯処罰が問題とされ得る余地がある。

例えば、既述のDavid Lennon事件との関係で示した英国の現行コンピュータ濫用禁止法では、故意（意図的）に結果を発生させた場合のみならず、過失（不注意）により結果を発生させた場合にも処罰可能となっていることから、英国においては理論上の問題というよりは現実の法解釈の問題になっているということができる。

これに対し、日本国の法令中には直接に適用可能な条項が存在しないように考えるのが一般的かもしれない。しかし、例えば、攻撃の標的となっているのが交通管制システムであるような場合、交通管制システムの誤作動や障害に

よって生じた死傷事故について、その誤作動や障害を発生させたDDoS攻撃のためのゾンビマシンとして使用されたPCの保有者についても過失致死傷罪の成否が問題となる余地を完全に否定し去ることができない。

この問題は、これまでほとんど論じられてこなかった問題であるし、とりわけゾンビマシンの保有者が営利企業や国などの公的機関である場合と全くの一個人である場合とで注意義務の程度・内容に差があるのかどうか等について慎重に検討がなされなければならない。[37] しかし、今日の社会では、良かれ悪しかれパブリッククラウドコンピューティングサービスを用いた業務処理が定着しつつあり、パブリッククラウドコンピューティングサービスを提供するベンダに注意義務違反があると、パブリッククラウドコンピュータ上に仮想的に構築される無数の仮想サーバをゾンビマシンとして一挙に極めて強力なDDoS攻撃を実行することが（少なくとも理論的には）可能であることから、今後、重要な検討課題として真剣に取り組まなければならない課題の一つであるということができる。

注

（1）この定義は、後述の欧州サイバー犯罪条約第二章第一節（刑事実体法）における定義に準拠するものである。

（2）二〇一〇年一〇月二四日から同月二六日までの間、ベルリンにおいて、「G8リヨングループ・ハイテク犯罪対策に関する政府・産業界合同ワークショップ」が開催された。
http://www.mofa.go.jp/mofaj/gaiko/summit/ko_2000/genoa/lyon.html［二〇一二年四月一五日確認］

（3）外務省『サイバー犯罪に関する条約』
http://www.mofa.go.jp/Mofaj/Gaiko/treaty/pdfs/treaty159_4a.pdf［二〇一二年四月一五日確認］
なお、条約原文（英文）及びその詳細説明書が欧州評議会（Council of Europe）のウエブサイトで公開されている。
http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG［二〇一二年四月一五日確認］

（4）外務省『サイバー犯罪に関する条約の説明書』（平成一六年二月）
http://www.mofa.go.jp/Mofaj/Gaiko/treaty/pdfs/treaty159_4b.pdf［二〇一二年四月一五日確認］

（5）　本稿は、論文としての基本的な骨格としては二〇一一年二月に限定会員向けメールマガジン誌上で公表した拙稿「DDoS 攻撃に適用可能な刑罰法令―比較法的検討」をベースとしつつ、その後のインターネット上でのサイバー攻撃の激化という社会情勢の変化並びに日本国及び主要各国立法動向等を踏まえ、ほぼ全面的に補正を加え、かつ、大規模に加筆した上で、新たな論文として公表するものである。

（6）　佐々木良一監修・日本ネットワークセキュリティ協会編著『情報セキュリティプロフェッショナル総合教科書』（秀和システム、二〇〇五年五月一〇日）五六一頁

（7）　Susan Hansche, John Berti, Chris Hare（笠原久嗣・大河内智秀・福島　聡監訳）『CCISP認定試験公式ガイドブック』（NTT出版、二〇〇五年九月一六日）二〇二頁

（8）　Dawn Cappelli, Andrew Moore & Randall Trzeciak, The CERT Guide to Insider Threats, Addison Wesley, January 2012, p.288

（9）　ゾンビマシンは、サーバとして用いられているコンピュータだけとは限らない。現実に発生した DDoS 攻撃の実例をみると、ノートPCを含め普通のPCを攻撃用のゾンビマシンとして利用した例が多数ある。今後は、いわゆるスマートフォンのような携帯電話型小型PCやタブレット型PCなども DDoS 攻撃のためのゾンビマシンとして用いられる可能性がある。

（10）　この誤作動の中にはIDやパスワードの照合処理も含まれる。そのため、無権限でサーバにアクセスするための手段として DDoS 攻撃が実行されることがある。

（11）　Will Gradigo & John Pirc, Cybercrime and Espionage - An Analysis of Subversive Multivector Threat, Elsevier, 2011, p.163

（12）　辻井重男監修『デジタル・フォレンジック事典』（日科技連、二〇〇六年一二月二〇日）一六五頁

（13）　「アノニマス」は、特定の者がリーダーとなった固定的な組織・団体であるとは考えにくい。むしろ、①既に「アノニマス」としてサイバー攻撃を実行している者または②その行為に共鳴する多数の者が、ムーブメントの一種として「アノニマス」を名乗った行動をとっていると考えたほうが妥当と思われる場合が多い。仮にそうであるとした場合、伝統的に考えられ想定されてきた「組織犯罪」という概念から相当かけ離れたものであることになることから、捜査手法にも根本的な見直しが迫られていると言える。他方で、「アノニマス」を名乗りながら、真実は単なる犯罪者集団または犯罪者個人による攻撃である場合がないとは言えないし、更に、特定の国家が「アノニマス」の行為に見せかけてサイバー戦の一部としての電子的な攻撃をしかけ

ているということがあり得ることにも留意すべきである。このような場合、本質的には警察所管の事柄ではなく国家防衛（自衛隊）所管の事柄であり得るわけであるが、現象としては同一の DDoS 攻撃がなされているようにしか見えないため、国防と警察との境界が判然としなくなるという困難な事態（戦時と平時が常に共存する状況）が生ずることになる。この種の困難に対処するための唯一の方法は、サイバー攻撃への対応として、自衛隊と警察との情報交換等の連携を強化するという方策を採用することが重要であると考える。

（14）　DDoS 攻撃の攻撃者が国や政治組織・政治団体であることもあり得る。インド、パキスタン、バングラデシュ等で頻発している DDoS 攻撃は、宗教対立を背景にしてはいるものの、実質的には国際紛争に類するタイプのものだと推定されており、いわばサイバー戦（Cyberwar）の一部となっていると理解するのが一般的である。なお、サイバー戦の概念については、Jeffrey Carr, Inside Cyberwarfare, O'Reilly, 2012 を参照されたい。

（15）　DDoS という攻撃手法は、ソヴィエトロシア当時にロシア海軍によって戦術として考案され、実際に戦闘訓練が実施された「対艦ミサイル飽和攻撃」にヒントを得たものとする見解がある。これは、米国の空母に対して対艦攻撃ミサイルによる攻撃をしかけようとする場合、対艦ミサイル迎撃用のミサイルが一〇〇パーセントの確率で命中したとしても、迎撃用ミサイルよりも一発でも多くの対艦攻撃ミサイルの数が多ければ迎撃ミサイルによる防御を無効にすることができる。そのことから、やや精度が劣っても相当多数の対艦攻撃ミサイルを同時に発射すれば、優秀でも非常に高価なために数に制限のある迎撃ミサイルを防御側で発射し尽くした後に、必ず何発かの対艦攻撃ミサイルを命中させることができるという考え方に基づくものである。「対艦ミサイル飽和攻撃」にヒントを得たものとする見解の当否を判定する能力はないが、客観的には、同種の発想に基づく攻撃手法であることを否定することができない。

（16）　Woody Leonhard (InfoWorld), New DoS tool from THC: Another overhyped threat, October 26, 2011 http://www.infoworld.com/t/security/new-dos-tool-thc-another-overhyped-threat-177167［二〇一二年四月一五日確認］

（17）　Mathew J. Schwartz (dark READING), DDoS Tools Aplenty On The Market For Hactivists, February 9, 2012 http://www.darkreading.com/security/vulnerabilities/232600597/ddos-tools-aplenty-on-the-market-for-hactivists.html［二〇一二年四月一五日確認］

（18）　一般的には「サービス妨害」と訳する例が多い。しかし、例えば、フロリダ州刑法の条文を読めば理解できるとおり、「妨害」と訳すると意味的な不都合が生ずることが明らかであり、「拒否」と直訳するのが正しい。

（19） 二〇一二年四月一五日時点で有効な条項

（20） California Penal Code
http://www.leginfo.ca.gov/cgi-bin/displaycode?section=pen&group=00001-01000&file=484-502.9［二〇一二年四月一五日確認］

（21） 現実には、攻撃者がその身元を隠し、捜査の手を逃れるため、自分が保有するマシンから直接に攻撃をしかけることはないだろうと推測される。自分が保有するマシンから直接に攻撃をしかけた場合、通信ログとＩＰアドレスの解析等により、簡単に攻撃者を特定できてしまうのが普通である。後述の David Lennon 事件の顛末からもそのことを理解することができる。

（22） 普通のインターネット利用者がインターネットを利用している際、突然、情報セキュリティ上の脆弱性があり危険である旨の警告が画面表示され、狼狽した利用者を偽セキュリティサイトに誘導した上で、偽セキュリティソフトをダウンロードさせてマルウェアに感染させる行為を俗に「スケアウェア（Scareware）」と呼んでいる。これは、利用者を怖がらせてダウンロードさせることから命名されたものとされている。

（23） DDoS 攻撃のための準備行為について、たまたま別の処罰法令の定める保護法益の侵害行為となるような場合の典型例の一つと言える。ただし、このような場合において、本来であれば刑法犯である業務妨害罪の一種として処罰すべきであるのに、準備行為または予備行為に対する処罰条項がないという理由で他の法令で処罰しようとすることに対する批判はあり得る。

（24） 岡村久道『情報セキュリティの法律』（商事法務、二〇〇七年七月九日）二三二頁

（25） この点について、米澤慶治編『刑法一部改正法の解説』（立花書房、一九八八年九月二〇日）一〇一頁は、不正の指令とは、「当該事務処理の場面において、与えられるべきでない指令のことである」と解説している。与えられるべきでない指令であっても、指令それ自体としては正常に処理可能なものでなければ実行不能となることから（このことは、サイバー法の専門家の間では常に物笑いの種となっている。）、この解説によっても条文それ自体の不適切さを補うことができない。更には、システムのテストのために、権限のあるエンジニアによって「虚偽の情報」が入力されることもしばしばある。つまり、刑法二三四条の二の立法における構成要件の選択には誤りがあると言わざるを得ない。正しくは、「無権限で情報または命令を」とするのが正しく、そのように法改正すべきである。なお、サイバー犯罪一般について、権限の有無を中心として理論を再構成すべきであることについては、夏井高人「アメリカ合衆国におけるコンピュータ犯罪立法動向―無権限アクセスを中心とする比較法的検討と日本法への示唆」判タ一〇〇八号一〇六頁。

(26)　この例では、第三者のログオン用ＩＤそれ自体は虚偽ではないので（虚偽のログオンＩＤである場合または現実には存在しないログオンＩＤである場合には、この例の方法による行為として限定的に理解する限り、不能犯となる。）、虚偽の情報を与えたことにならない。そして、コンピュータシステムの処理能力が非常に高く、最初のログオンが成功した後の重複ログオンを何らの支障もなく排除してしまった場合、DDoS 攻撃としては失敗したことになるが、第三者のＩＤを無権限で用いたのである以上、電子計算機損壊等業務妨害罪とは別に不正アクセス罪が成立することになる。

(27)　器物損壊罪の罪質及び既遂時期等については議論の余地がある。とりわけ、器物損壊罪の保護法益について器物の効用であるとの見解を採用した場合、特定の器物を手段として提供される役務の保護と器物それ自体としての効用との間の境界が不鮮明となることがあり、処罰範囲が必要以上に拡張されてしまう危険性がある。

(28)　前掲『大コンメンタール刑法』一五八頁

(29)　筆者（夏井高人）が翻訳。以下、いずれも二〇一二年四月時点で有効なドイツ刑法の条文。

(30)　ドイツ刑法三〇三条ａ第一項（StGB § 303a Abs. 1）は、データ（電磁的記録）の改変行為を処罰するものである。

(31)　ドイツ刑法二〇二条ａ第二項（StGB § 202a Abs. 2）は、無権限のアクセスから保護されたデータ（電磁的記録）であって、電子的、磁気的その他の方法で送信または記録されたものをいうと規定している。日本国の刑法七条の二に定める「電磁的記録」の定義とは多少異なる。

(32)　法務大臣官房司法法制調査室編『ドイツ刑法典』（法曹会、一九八二年三月五日）の訳による。

(33)　過去において、現実にゲームソフトの中にコンピュータウイルスが混入していることに気づかずそのまま出荷してしまったという事例が存在する。この事例は、二〇〇一年一一月一五日にＣＤ－ＲＯＭ媒体で発売されたセガ社の家庭用ゲーム機であるドリームキャスト用ＲＰＧゲームソフト『マリー&エリーのアトリエ～ザールブルグの錬金術士１・２～』の中にコンピュータウイルス W32/Kriz が感染していたというものだった。このコンピュータウイルスは、非常に大きな破壊力を有するものであり、ゲームソフト開発中に開発担当エンジニアのＰＣから感染したものと推定されている。

(34)　Spanish hacker sentenced to two years in jail for DDoS attack
Sophos: February 7, 2006
http://www.sophos.com/ja-jp/press-office/press-releases/2006/02/garrido.aspx［二〇一二年四月一五日確認］

(35)　Director of Public Prosecutions v David Lennon [2006] EWHC 1201

http://www.bailii.org/ew/cases/EWHC/Admin/2006/1201.html［二〇一二年四月一五日確認］

（36） ［訳注］対象について概括的または抽象的な認識で足りるということを意味している。したがって、具体的に特定のコンピュータシステム、コンピュータプログラムまたはコンピュータデータを認識していなくても、何らかのコンピュータシステム、コンピュータプログラムまたはコンピュータデータとの関係で行為を実行しているという認識があれば犯罪が成立することになる。

（37） 例えば、一市民がウイルス検知ソフトをノートＰＣにインストールして警戒していなかった場合、当該ノートＰＣがゾンビマシンとして利用されたことについて注意義務違反があったかどうかが問題となり得る。