

高度情報化社会におけるサイバー犯罪に関する論考

— その概念と手法を中心に —

成 鈴 木 耆 政
田 中 尚 通
葛 西 正 敏
 和 敏
 広

A Study on Meanings and Techniques of Cybercrime in Advanced Information Society

*Kijung SUNG, Naomichi SUZUKI,
Masatoshi TANAKA and Kazuhiro KASAI*

目 次

- I. はじめに—サイバー犯罪の登場背景—
 - II. サイバー犯罪に関する概念的整理
 - 1. サイバー犯罪の概念
 - 2. サイバー犯罪の特徴
 - III. 日本におけるサイバー犯罪の現況
 - 1. サイバー犯罪の検挙状況
 - 2. 検挙事件からみたサイバー犯罪の特徴
 - 3. サイバー犯罪等に関する相談状況
 - IV. サイバー犯罪の類型と手法
 - 1. システム関連サイバー犯罪の類型と手法
 - 2. 一般的サイバー犯罪の類型と手法
 - V. おわりに—サイバー犯罪への対策—
- 【註】
【参考・引用文献】

I. はじめに—サイバー犯罪の登場背景^{註1)}

昨今、パーソナルコンピュータ（PC）の急速な普及と情報通信技術（ICT；Information and Communication Technology）^{註2)}の結合により、インターネットが日常生活において欠かすことのできない重要なツールとして登場したことで、サイバースペースが新しい生活空間として定着しつつある。すなわち、コンピュータネットワークとしてのインターネットを利用することでサイバーショッピング（インターネットショッピング）^{註3)}、サイバー金融（インターネットバンキング）、株取引、電子メールによるコミュニケーション、インターネットによる届出・書類申請などほとんどすべてのことを処理し、必要な情報に対しても時間的・空間的制約なしで容易にアプローチすることができるようになった。

このようなサイバー空間という新しい生活空間の登場は必然的に新しい形態の犯罪類型を誘発し、2000年2月には何者かによって世界最大のインターネット検索サイトともいえるyahoo^{註4)}を始め、buy.com^{註5)}、eBay^{註6)}、Amazon.com^{註7)}、zdnet^{註8)}、etrade^{註9)}、CNN.comなどアメリカの大手有力ポータルサイトがDDoS（Distributed Denial of Service）攻撃^{註10)}を受け、数時間ずつアクセス不能な状態に陥った事件があった。日本においても、2000年1月にクラッカーが省庁ウェブサイトに連続して侵入し、情報を改ざん・破壊する事件が発生し、危機感の希薄な日本の現状を浮き彫りにした^{註11)}。そして、世界各国でさまざまなサイバー犯罪が犯され、その対策として法規制を始めとする諸般措置に追われている。しかしながら、サイバー空間を利用する新しい犯罪のほとんどは、既存の法規が対応できない側面を持ち、立法的装置と制度的補完などの努力にもかかわらず、サイバー犯罪は増加趨勢にある。このようなサイバー犯罪増加の原因の一つとして、サイバースペースの特徴を挙げることができる。すなわち、サイバー空間は地理的、時間的に無制約で、匿名性、無痕跡性、不特定多数性など現実空間とはその特性に違いがあるため、サイバースペースと現実空間との間には、物理的にも意識的にも大きなギャップが生じている。このギャップの存在こそが犯罪者に付け入る隙を与え、サイバー犯罪増加の原因になっているともいえる^{註12)}。

以上のことをふまえ、本稿ではサイバー犯罪の概念的整理と日本におけるサイバー犯罪の現況、サイバー犯罪の類型と手法、そしてその対策などの考察を目的とした。

II. サイバー犯罪に関する概念的整理

1. サイバー犯罪の概念

1-1 サイバー空間の定義

一般的にサイバー空間（cyberspace）^{註13)}とは、コンピュータ通信網をつうじたネットワークでつながっている空間のことで、インターネットとコンピュータ通信など通信網で構築された情報交換・共有の場のことである。すなわち、仮想現実（virtual reality）、人工現実（artificial reality）とも表現され、物理的には存在しないが、多くの人が感じたり、対話したり、商品の取引なども行われる世界（空間）のことである。これは全世界的につ

ながっているネットワークシステムで構成された仮想サービス空間として、無形の空間を意味する。

このようなサイバー空間と呼ばれる仮想空間はただ見えない空間であって存在しない空間ではなく、実際には我々の実生活と密接な関係を持っている空間として、現実社会の法の適用の枠組みの中で運用されるべきであろう。したがって、サイバー空間で行われている諸般事項を明確に認識し、これに対する法的判断基準とサイバー空間の安全と秩序確立を図ることは今日のような高度情報化社会において何よりも重要な課題であろう。

1-2 サイバー犯罪の定義

サイバー犯罪 (cybercrime) という用語は比較的最近になって使用し始めたもので、その概念的な定立は未だなされておらず、一般的にサイバー空間 (cyberspace) で発生する犯罪を総称する概念として用いられている。サイバー犯罪という用語に対する最近の傾向をみると、サイバー空間と関連して起こる犯罪行為、ないし反社会的行為を総称する意味合いで使われている。

Parker (1998)^{註14)}はサイバー犯罪について、サイバー空間に対する特別な知識を用いた犯罪と少々曖昧な定義づけをしている。事実、彼はサイバー犯罪をただサイバー空間という新しい道具と目標を使用する、すなわち新しい環境の中で発生する点を除けば、現実世界で発生する犯罪と本質的に同じであると述べている。また、Thomas (2000)^{註15)}はサイバー犯罪を、コンピュータと全世界的な電子ネットワークを媒介にした不法的、または不法的なものとして見なしうる行為、または活動であると定義づけている。

警察庁の資料^{註16)}によると、サイバー犯罪とは、2001年11月に日本を含む30カ国が署名した「欧州評議会サイバー犯罪に関する条約 (Cybercrime Convention)」^{註17, 18)}の定義、すなわち不正アクセス (illegal access)、不正な傍受 (illegal interception)、データの妨害 (data interference)、システムの妨害 (system interference)、装置の濫用 (misuse of devices)、コンピュータに関連する詐欺 (computer-related fraud)、コンピュータに関連する偽造 (computer-related forgery)、そして児童ポルノに関連する犯罪 (offenses related to child pornography) などの「情報技術を悪用した犯罪」を意味し、すでに国際的に定着した用語となっている。この資料ではサイバー犯罪について「コンピュータ技術および電気通信技術を悪用した犯罪の総称」と定義しているが、詳しくは次の三つの類型に分類することができる。まず第一に、コンピュータ、電磁的記録対象犯罪である。これは刑法に規定されているコンピュータや電磁的記録を対象とした犯罪のことを意味する。その主な例としては、①金融機関などのオンライン端末を不正操作し、無断で他人の口座から自分の口座に預金を移した行為 (電子計算機使用詐欺罪)、②サーバーコンピュータに保存されているウェブページのデータを無断で書き換える行為 (電子計算機損壊等業務妨害罪)、そして③ウイルスに感染したファイルを送信し、他人のコンピュータをウイルスに感染させ、正常に使用できない状態にした行為 (器物損壊罪) などが挙げられる。

第二に、ネットワーク利用犯罪である。これは上述の第一以外で、犯罪の実行にネットワークを利用した犯罪、または、犯罪行為そのものではないものの、犯罪の敢行に不可欠な手段としてネットワークを利用した犯罪のことをいう。主な例としては、①電子掲示板に販売広告を掲示し、覚せい剤などの違法な物品を販売する行為、②インターネットオー

クションで、自分が所有していない品物を出品し、落札者から代金をだまし取る行為、③インターネットに接続されたサーバーコンピュータにわいせつな映像を置き、これを多くの人に対して閲覧させる行為、④掲示板でネズミ講、賭博、宝くじの購入などを勧誘する行為、⑤特定個人の誹謗中傷記事をウェブページや掲示板に掲載する行為、そして⑥脅迫恐喝電子メールを送付する行為など、犯罪の実行にあたりネットワークを利用した場合をいう。

第三に、不正アクセス行為の禁止などに関する法律違反である。その主な例としては、①不正アクセス行為、すなわち、他人の ID、パスワードなどを無断で使用し、ネットワーク越しにコンピュータを不正使用する場合（なりすまし行為）、不正なプログラムを使用するなどし、コンピュータの安全対策上の不備（セキュリティ・ホール）を突き、ネットワーク越しにコンピュータの管理者権限を不正使用した場合（セキュリティ・ホール攻撃）と、②不正アクセス助長行為、すなわち、コンピュータを利用するための ID、パスワードなどをユーザーに無断で第三者に教える場合などが挙げられる。

Goodman^{註19)}によると、サイバー犯罪とは一つ、またはそれ以上のコンピュータを用いて行う犯罪のことで、コンピュータが犯罪の目的となったり、犯罪の道具として用いられ、またはコンピュータと関連して副次的に発生するなどの三つの範疇に分類している。

最近にはコンピュータネットワークと関連した犯罪を通称してサイバー犯罪と呼ぶ傾向にある。サイバー空間で発生するコンピュータ関連犯罪については、サイバー犯罪という表現以外にもコンピュータ犯罪、インターネット犯罪、電算網犯罪、ネットワーク犯罪、ハイテック犯罪、情報通信犯罪、そして情報犯罪など多様な用語が使われている。ここでは一般的に用いられているが、サイバー犯罪とは少し異なる概念であるコンピュータ犯罪、情報犯罪、そしてハイテック犯罪の概念を比較・検討することでサイバー犯罪の概念を明確にしたい。

1-3 コンピュータ（関連）犯罪（computer related crime）

コンピュータ犯罪の概念については現在一致した定義づけはなされておらず、一般的にコンピュータ犯罪とはコンピュータの機能を利用した犯罪現象、またはコンピュータの機能やコンピュータと関連した電子的資料を犯行の対象とする犯罪現象を意味している。

警察庁ではコンピュータ犯罪をコンピュータシステムに係わった犯罪、またはこれを悪用する犯罪^{註20)}と定義づけ、経済産業省ではコンピュータ犯罪について、コンピュータが直接的に、または間接的な形で介在した社会悪行為であると定義づけている。また、Bequai^{註21)}は財やサービスの取得、または政治的、経済的利益を得るための欺罔（相手を錯誤に陥らせるように事実をいつわること）、隠蔽、偽装行為などにコンピュータを使用することであると定義づけている。安富^{註22)}は、コンピュータ犯罪という用語は1987年の刑法一部改正の際に定義されており、コンピュータ、もしくは電磁的記録を対象とした犯罪、システム機能の阻害、不正使用のことを指すとしている。すなわち、これはネットワークそのものより、システムに重点を置いた概念づけであるといえる。

コンピュータ犯罪という用語は、その概念の中に既にコンピュータ不正操作（computer manipulation）^{註23)}、データの不正入手、ないしコンピュータスパイ（computer spy, com-

puter espionage)^{註24)}、コンピュータ破壊^{註25)}、ないしコンピュータ業務妨害 (computer sabotage)、そしてコンピュータ無権限使用 (time theft, service theft)^{註26)}とプライバシー侵害などの類型が含まれている^{註27)}。

今日、コンピュータ性能の発展と急速な普及により財産領域のみならず、コンピュータが使用されるほとんどすべての領域で侵害行為が現れているといっても過言ではない。コンピュータ犯罪は経済的な領域のみならず、プライバシー侵害など多様な領域で侵害をもたらし、またコンピュータとインターネットをつうじた多様な犯罪の可能性が開かれている状況である。したがって、コンピュータ犯罪の概念を広義の概念としてとらえ、コンピュータが行為の手段ないし目的であるすべての種類の社会侵害的行為として把握すべきであろう。

1-4 情報犯罪 (information crime)

情報犯罪とは、情報社会において問題点として取り上げられている情報現象の中で代表的なものといえる情報処理装置、または情報を利用する犯罪、そして情報処理装置、または情報に対する犯罪を総称する用語である。しかしながら、情報に対する犯罪を総称するということはサイバー空間とは関連なく起こる情報に対する不法的な探索、漏洩行為、盗聴行為、他人間の対話の録音、聴取、または取得する行為も考慮の対象にしなくてはならない問題が生じる。

1-5 ハイテック犯罪 (high-tech crime)

ハイテック犯罪とは高度科学技術、または先端科学技術と関連性のあるすべての新種犯罪を指す用語である。しかし、高度科学技術、または先端科学技術と関連性のあるすべての犯罪をハイテック犯罪と呼ばれているが、科学技術の中でもコンピュータ技術および情報通信技術、または両者の結合として形成される仮想空間と直接関連のある犯罪類型をハイテック犯罪という。

アメリカのカリフォルニアに本部を置いてある国際高級技術犯罪調査協会 (HTCIA; International High Technology Crime Investigation Association)^{註28)}の内規ではコンピュータおよび科学技術と両方に関連している、またはある一方と関連のある犯罪行為をハイテック犯罪と規定している。そして、アメリカのワシントン州に本部を置いてあるハイテック犯罪コンソーシアム (High-Tech Crime Consortium)^{註29)}の内規はコンピュータを不法行為の道具、または犯罪行為の目的物として利用した犯罪事件をハイテック犯罪として規定している^{註30)}。しかし、ハイテック犯罪は、高度の科学技術ないし先端科学技術を使用する犯罪という意味が含まれていて、サイバー空間での犯罪行為を総称するにはその意味上限界があるといえよう。

2. サイバー犯罪の特徴

サイバー犯罪の特徴としては、まず第一に、サイバー空間の匿名性と非対面性を挙げることができる。サイバー空間はコンピュータを利用したネットワークを媒介に形成する空間で、不可視的で現実世界とは異なり、行為者が自らの顔 (身分) を現さずに行動する、または電子商取引のように直接対面しない非対面的活動という特徴を持っている。した

がって、サイバー空間でのすべての犯罪行為も姿を現さない状態で他人の ID を盗用したり、犯行を隠蔽したりすることも可能である。また、サイバー犯罪の非対面性により犯罪者はより過激で大胆な行動（犯行）を犯す場合が多い。

そして、サイバー犯罪の匿名性と非対面性の特徴により、捜査機関の立場からみると、犯人の現場性が欠如され、痕跡を容易に消すこともできるサイバー犯罪の特性上、犯罪者の検挙が困難になるケースも多い^{註31)}。

第二に、専門性と技術性が挙げられる。サイバー犯罪の中には、コンピュータとインターネットに対する若干の知識と技術があれば犯すこともできるものの、コンピュータプログラム操作をつうじた財産取得、ウイルス製作および流布、ハッキングのようなサイバー犯罪は高度の専門的な知識と技術を備えることで可能な犯罪が大部分である。

第三に、時空間超越性（無制約性）が挙げられる。インターネットは TCP/IP^{註32)} という共通の通信規約を用いて、全世界のコンピュータ通信網を一つの集合体としてつないでいることで、国家間の境界および地理的制約を解消することができる。このようなインターネット空間の時空間無制約性は潜在的な犯罪者に多くの犯罪の機会を提供しているともいえる。

第四に、即時性を挙げることができる。サイバー空間の基本的なコミュニケーション手段であるインターネットはただ一回のクリックで相手との意志疎通を可能にすることで、ユーザーは深刻に考えずに特定、または不特定多数に直接情報を発信することができる。これは、サイバー空間のメンバーは現実世界より容易に相手と接触でき、メッセージ伝達の公的性格が相対的に弱いことを意味する。このような特徴により、現実世界よりサイバー空間での反倫理的行為や犯罪行為がより容易に発生するともいえる。

そして第五に、双方向性が挙げられる。インターネット、特に WWW サービスを用いる場合に現れる最も大きな特徴は、相互対話式双方向サービスが可能である点である。チャット、電子メール、そしてニュースグループなどはユーザーに対話を提供するコミュニケーションの双方向的タイプといえる。このような特徴はアダルトサイトや危険情報サイト（集団自殺サイト、殺人請負サイトなど）の開設を可能にし、チャットによるネット売春行為も可能にしている。

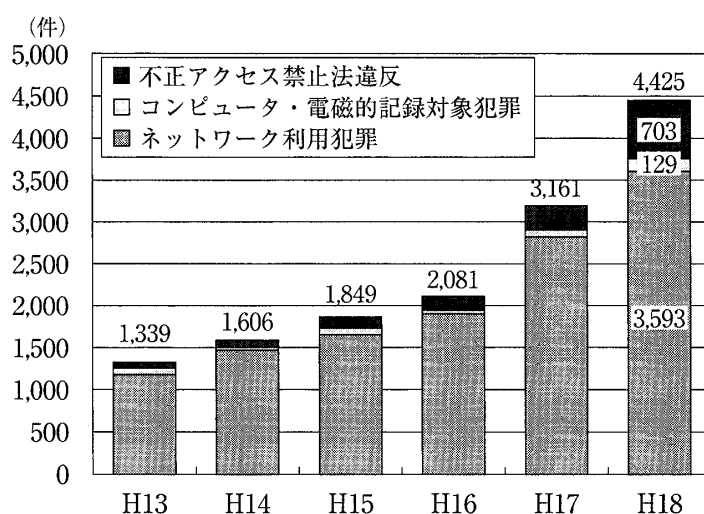
Ⅲ. 日本におけるサイバー犯罪の現況^{註33)}

1. サイバー犯罪の検挙状況

高度情報通信ネットワーク社会の光の部分が進展するに伴い、その陰の部分も露呈しており、サイバー犯罪の驚異的な増大は、大きな社会問題となっている。

2006年中のサイバー犯罪、すなわち情報技術を利用する犯罪の検挙件数は4,425件で前年（3,161件）より40.0%増加している。これは、2001年から5年間でサイバー犯罪の検挙件数が約3.3倍になったことを示し、今後、年々増加すると予想される（図表1, 2, 3）。ここでサイバー犯罪の内訳別に少し述べてみると次のとおりである。まず第一に、不正アクセス禁止法違反である。サイバー犯罪のうち、不正アクセス禁止法が施行された2000年から一貫して増加し、2006年の不正アクセス禁止法違反は703件、検挙人員は130人で、前

<図表1> サイバー犯罪検挙件数の推移



出所: 「平成18年のサイバー犯罪の検挙及び相談状況について」『広報資料』警察庁, 2007年2月22日。

<図表2> サイバー犯罪の検挙状況

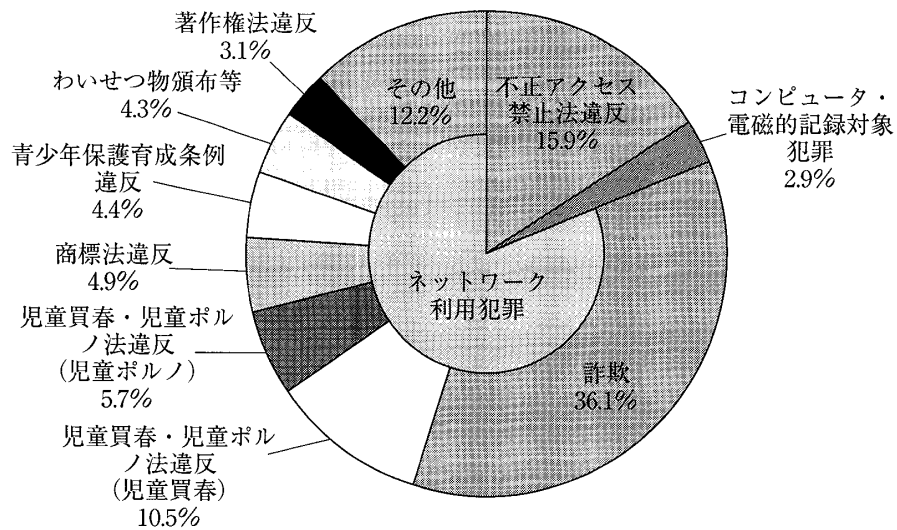
罪 名 \ 年度	H13	H14	H15	H16	H17	H18	増 減
不正アクセス禁止法違反	67	105	145	142	277	703	+ 426 (+153.8%)
コンピュータ・電磁的記録対象犯罪	63	30	55	55	73	129	+ 56 (+ 76.7%)
電子計算機不正使用詐欺	48	18	34	42	49	63	+ 14 (+ 28.6%)
電磁的記録不正作出・毀棄	11	8	12	8	17	56	+ 39 (+229.4%)
電子計算機破壊等業務妨害	4	4	9	5	7	10	+ 3 (+ 42.9%)
ネットワーク利用犯罪 ^{注1)}	1,209	1,471	1,649	1,884	2,811	3,593	+ 782 (+ 27.8%)
詐欺	485	514	521	542	1,408	1,597	+ 189 (+ 13.4%)
児童買春・児童ポルノ法違反(児童買春)	117	268	269	370	320	463	+ 143 (+ 44.7%)
児童買春・児童ポルノ法違反(児童ポルノ)	128	140	102	85	136	251	+ 115 (+ 84.6%)
商標法違反	31	37	95	82	109	218	+ 109 (+100.0%)
青少年保護育成条例違反	10	70	120	136	174	196	+ 22 (+ 12.6%)
わいせつ物頒布等	103	109	113	121	125	192	+ 67 (+ 53.6%)
著作権法違反	86	66	87	174	128	138	+ 10 (+ 7.8%)
その他 ^{注2)}	249	267	342	374	411	538	+ 127 (+ 30.9%)
合 計	1,339	1,606	1,849	2,081	3,161	4,425	+1,264 (+ 40.0%)

注1): ネットワーク利用犯罪の定義: 犯罪の構成要件に該当する行為についてネットワークを利用した犯罪, または構成要件該当行為でないものの, 犯罪の実行に必要不可欠な手段としてネットワークを利用した犯罪をいう。例えば, 児童買春については, ネットワーク上で連絡を取り合った者同士がネットワーク上において児童買春に合意し, 児童買春に及んでいる場合に限り計上しており, 青少年保護育成条例違反についても, これと同様の考え方に基づいて計上している。

注2): その他には, 名誉毀損, 脅迫, 覚せい剤取締法違反等の薬物事犯, 銃砲刀剣類所持等取締法, 売春防止法, 児童福祉法等の違反がある。

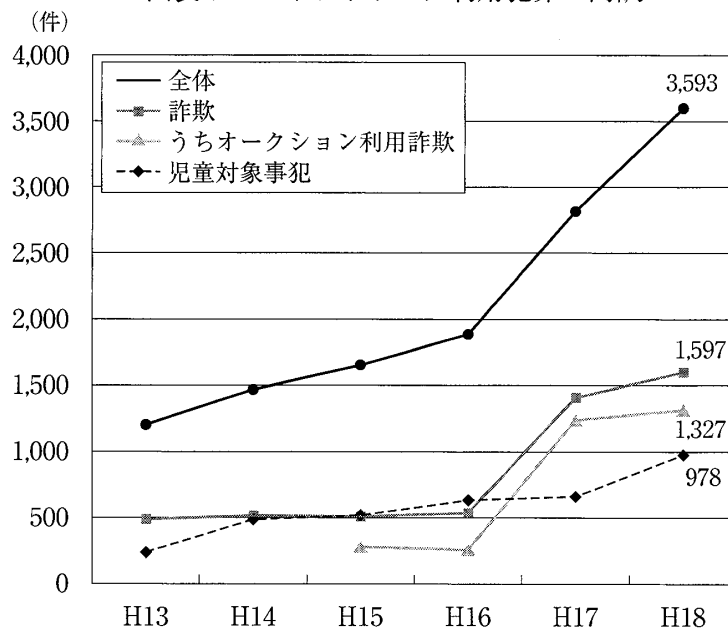
出所: <図表1>と同じ。

＜図表 3＞ サイバー犯罪の罪名別の割合（2006年）



出所：＜図表 1＞と同じ。

＜図表 4＞ ネットワーク利用犯罪の内訳



出所：＜図表 1＞と同じ。

年（277件，113人）の約2.5倍に増加している。その内訳をみると，不正アクセス行為に係わるものがそれぞれ698件，130人，不正アクセス助長行為^{註34）}に係わるものがそれぞれ5件，5人であった。

第二に，ネットワーク利用犯罪である。ネットワークを利用した犯罪は，サイバー犯罪の検挙件数のうち最も多くを占める犯罪であり，2006年中は3,593件，前年（2,811件）より27.8%増加している（図表 4）。

第三に，コンピュータ・電磁的記録対象犯罪である。コンピュータ，または電磁的記録

を対象とした犯罪は129件で、前年（73件）より76.7%の増加を示している。

2. 検挙事件からみたサイバー犯罪の特徴

検挙事件からみたサイバー犯罪の特徴としては、まず第一に、インターネット・オークション詐欺の多発である。2006年のネットワーク利用の詐欺の検挙件数は1,597件で、ネットワーク利用犯罪の全検挙件数の44.4%を占めている。この中で83.1%がインターネット・オークションに係る詐欺である。

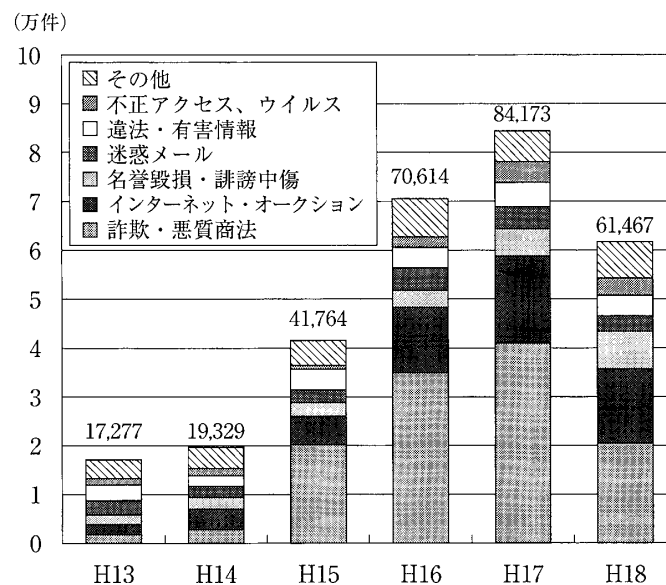
第二に、児童の性的被害に係る犯罪の増加を挙げることができる。2006年の児童の性的被害に係る犯罪、すなわち、児童買春・児童ポルノ法違反、青少年保護育成条例違反および児童福祉法違反の検挙件数は978件で、前年（666件）の約1.5倍に増えている。

第三に、犯行の組織化・高度化の傾向である。インターネットを利用した共犯者の募集や他人名義口座の調達、フィッシング^{註35)}によりユーザーの設定・管理の甘さにつけ込んでID・パスワードの入手など、サイバー空間の特性を悪用した犯行の組織化、高度化の傾向がうかがわれる。

3. サイバー犯罪等に関する相談状況

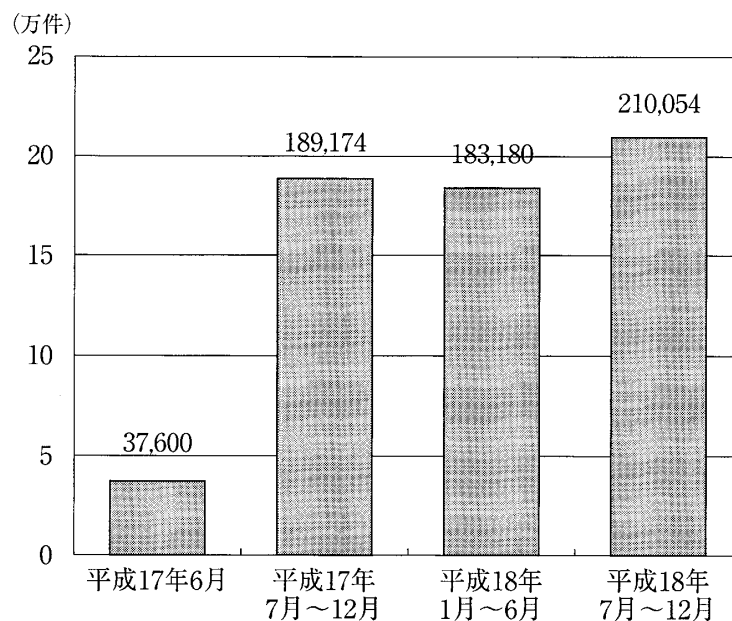
2006年中に都道府県警察の相談窓口で受理したサイバー犯罪などに関する相談件数は61,467件で、前年（84,173件）と比べて27.0%の減少を見せている。この中で減少の多くはワンクリック請求（詐欺）^{註36)}を中心とする「詐欺・悪質商法」である。一方、2006年中の「インターネット安全・安心相談システム」へのアクセス数は393,234件（1日平均1,077件）で、質問項目別では「料金請求」へのアクセスが全項目の54.1%（2006年4月～12月分の集計）を占めている（図表5、6）。

＜図表5＞ サイバー犯罪などに関する相談受理件数の推移



出所：＜図表1＞と同じ。

＜図表 6＞ インターネット安全・安心相談システムへのアクセス件数の推移



出所：＜図表 1＞と同じ。

4. サイバー犯罪の対する警察庁の対策

サイバー犯罪の対する警察庁の対策としては、まず第一に、サイバー犯罪に対する捜査力の強化を挙げることができる。その主な内容としては、高度なサイバー犯罪に対する最先端の捜査技術・捜査手法の開発、警察署における第一次的な対応能力の強化、そして事件の広域化に対応した合同・共同捜査の推進などである。

第二に、インターネット上におけるプレゼンスの強化を挙げることができる。その主な内容は、買受け捜査^{註37)}の推進と事件検挙時の広報の積極的な実施、違法・有害サイトのユーザーに対する警告の実施などである。

第三に、情報セキュリティに関する広報・啓発活動の推進が挙げられる。その主な内容としては、事業者、団体などとの連携による違法・有害情報の危険性の周知、児童の携帯電話へのフィルタリング導入の促進、そしてインターネットカフェに対する防犯指導の強化などである。

Ⅳ. サイバー犯罪の種類と手法

ここではサイバー犯罪の種類と手法^{註38, 39)}（図表 7）について、大きくシステム関連サイバー犯罪と一般的サイバー犯罪に分けて述べることにする。

1. システム関連サイバー犯罪の種類と手法

1-1 ハッキング (hacking)

ハッカー (hacker) とは、元々、コンピュータに情熱を持ち、コンピュータシステムの内部構造や動作原理などについて熱心に知ろうと努力する人のことを意味する。ここで

RFC1983/FYI18のInternet User's Glossaryの提案を受け入れると、ハッカーとは、システム、特に、コンピュータやコンピュータネットワークの内的な働きを深く理解することに喜びを覚える人（A person who delights in having an intimate understanding of the internal workings of a system, computers and computer networks in particular）のことを指す。

しかし、最近では、クラッカー（cracker）^{註40)}やシステム侵入者（system intruder）、窃盗犯（thieves）、コンピュータ破壊者（computer vandals）、知能型侵入者（uebecracker）、サイバーテロリスト（cyber terrorist）、そしてネットワークスパイ（network spy）などの否定的な意味で用いられている^{註41)}。ここではハッキングの主な技法（手段）^{註42)}について簡略に述べることにする。

第一に、サービス拒否攻撃（denial of service attack）である。インターネットでのサービス拒否（サービス不能、サービス妨害）攻撃^{註43)}とは、行為者がコンピュータシステムの正常的なサービスを妨害する目的で洪水（flooding）のように大量のデータパケットを送信し、対象ネットワークやシステムの性能（能力）を急激に低下させ、攻撃対象システムの提供するサービスを利用できないようにする攻撃のことで、ハッキング手法の中で最も一般的な方法である。

このような方法は、インターネットユーザーの少なかった初期は、単一システムやサービスを目標とする攻撃者と被害者が1：1の類型が多かったが、最近ではDDoS（Distrib-

<図表7> サイバー犯罪の類型（サイバー攻撃の手法）

サイバー攻撃 手法・ツール	攻撃・感染 経路・手法	攻撃・感染 対 象	発症時期	症状	犯罪被害
クラッキング ツール Exploitコード Dos, DDoS ウイルス ワーム トロイの木馬 rootkit スパイウェア ボットネット スパム スパイメール Cookie悪用 盗聴 なりすまし	(脆弱性) (ファイアウォール) リモートアクセス WEBアクセス (HP, 掲示板等) P2Pネット インスタント メッセンジャー チャット(IRC) メール送付 メディア送付 (CD-ROM)	デバイス・BIOS OS ブートセクタ DLL レジストリ アプリケーション ファイル データベース DNS, DDNS FW・SW	即時 自動 手動 (別命ある まで待機) 時限(条件) 爆弾	システム ダウンや 機能低下 意図しない 動作 他への攻撃 (DoS, 掲示板書込) 更なる 感染拡大 “踏み台”, “ボット”化 情報漏えい データの 消去・改ざん	不正アクセス 電磁的記録不正 作出・供用・毀棄 電子計算機損壊 等業務妨害 偽計・威力業務妨害 電子計算機利用詐欺 詐欺 誹謗中傷・名誉毀損 脅迫・ストーカー 自殺幇助 児童買春・ポルノ 児童福祉法違反 売春防止法違反 わいせつ物頒布等 青少年保護 育成条例違反 著作権法違反 商標法違反 賭博・富籤 薬物等取引 銃砲刀剣等売買
ITツール, サービス利用	あらゆるITメディア, サービス等 (例) 携帯電話, 無線LAN, ネットオークション, 掲示板・ブログ, SNS 出会い系サイト ダイヤルQ2, IP電話				
犯罪者・組織による悪用	暗号・認証技術等				

出所：羽室英太郎『サイバー犯罪・サイバーテロの攻撃手法と対策』立花書房，2007年4月，26頁。

uted Denial of Service；分散サービス拒否）攻撃といい、 n 個の不特定システムにより単一ネットワークを対象に攻撃を行う $n:1$ 類型が主である。

第二に、電子メール爆弾（E-mail bomb）である。電子メール爆弾とは、ある電子メールユーザーの電子メールプログラムを麻痺させる、または他の正当なメッセージの受信を妨害する意図で、そのユーザーの電子メールアドレスに一時的に大量の電子メールデータを発送する行為、またはこれにより発送されたデータのことをいう。すなわち、自動的に生成される内容とヘッダーを持つ電子メールをユーザーが指定した回数に発送するプログラムを利用し発送したり、大容量のファイルを添付し数回発送する、または攻撃対象ユーザーを多くの電子メールグループに加入させ同時に多くの電子メールを受信するようにすることでシステムをダウンさせる方法である。

第三に、論理爆弾（logic bomb）である。論理爆弾とは、一定の条件が満たされるとコンピュータを破壊する一種の悪性プログラムのことである。すなわち、特定の日付、時間など一定の条件を充足させるとコンピュータの情報を削除したり、インターネットなどのオンライン情報利用を阻害する特殊プログラムが自動的に作動し妨害する方法である。

第四に、トロイの木馬（trojan horses）である。トロイの木馬とは、正常的に機能するプログラムに仮装し、プログラムの中に隠れて意図しない機能を遂行^{註44)}するプログラムコードのことである。すなわち、これは資料の削除・情報の奪取などのサイバー犯罪を目的に用いる悪性プログラムである。これは、ハッキングの機能を持ち、インターネットをつうじて感染されたコンピュータの情報を外部に流出させることが大きな特徴である。しかし、プログラムのエラーであるバグ（bug：小さな虫）とは異なり、故意に浸透させられた点が特徴で、また自らを複製しない点でウイルスとも異なり、該当ファイルを削除することで治療が可能である。

トロイの木馬の代表的なプログラム^{註45)}としては、Back Orifice^{註46)}、NetBus^{註47)}、Deep Throat^{註48)}、Sub7^{註49)}、Worm Explore Zip, Pretty Park^{註50)}、Hot Keys Hook, Ecokys, Y2K, Mellisa, July Killerなどを挙げることができる。

第五に、インターネットワーム（internet worm）である。インターネットワームはネットワークに侵入しコンピュータ、ネットワーク、そしてユーザーに対する情報を入手した後、他のシステムのソフトウェア的な脆弱点を利用し該当システムに浸透し自分のコピーを作り、また他のシステムに移ることで、コンピュータの正常な作動を妨害しネットワークを麻痺させるものである。

1-2 コンピュータウイルス（computer virus）

コンピュータウイルスとは、第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラムのことであり、次の機能の一つ以上有するもののことである^{註51)}。

第一に、自己伝染機能である。自らの機能によって他のプログラムに自らをコピー、またはシステム機能を利用して自らを他のシステムにコピーすることにより、他のシステムに伝染する機能である。第二に、潜伏機能である。発病するための特定時刻、処理回数などの条件を記憶させて、条件が充足するまで症状を出さない機能である。第三に、発病機能である。プログラム、データなどのファイルの破壊を行ったり、設計者の意図しない動

作をさせるなどの機能である。

すなわち、コンピュータウイルスとは、プログラマが意図的にコンピュータシステムを破壊したり、ファイルを削除するなどの破壊作用をするように作られたもので、自己コピーを行って伝播したり、システムへの誤作動、ファイルの損傷を起こすプログラムのことである。ここではコンピュータウイルスの感染経路^{註52)}について述べることにする。

第一に、電子メールの添付ファイルを挙げることができる。ウイルスの感染経路として最も一般的なのは、電子メールの添付ファイルによるものである。電子メールの添付ファイルとして送信されたウイルスを実行することで、そのウイルスに感染してしまうようになる。

第二に、電子メールのHTML スクリプトである。添付ファイルが付いていない電子メールでも、HTML メールであればウイルスを送信することができる。すなわち、HTML メールはウェブページと同じように、メッセージの中にスクリプトと呼ばれるプログラムを挿入することができるので、ウイルスを侵入させることが可能である。

第三に、ウェブページの閲覧が挙げられる。ウェブブラウザは、ウェブページでさまざまな処理ができるように、JavaScript^{註53)}やVBScript^{註54)}、ActiveX コントロール^{註55)}、Java^{註56)}などのプログラムが実行可能になっている。そのために、これらのプログラムでウイルスが埋め込まれたウェブページを閲覧した場合、ウイルスに感染するケースが多い。

第四に、ネットワークにおけるファイルの共有である。ウイルスによっては、感染したコンピュータに接続されているファイル共有用のネットワークドライブを探し出し、特定の拡張子を持つなど、ある一定の条件で探し出したファイルに感染するタイプのものがある。この種類のウイルスは企業内ネットワークを経由し、他のコンピュータやサーバーにも侵入する可能性もある。

そして第五に、マクロプログラムの実行が挙げられる。これは Office アプリケーションのマクロ機能を利用し感染するウイルスである。これらは、マクロウイルス (macro virus) と呼ばれているが、Office アプリケーションのマクロ機能では、プログラム開発言語である VBA (Visual Basic for Applications)^{註57)}を用いるため、ファイルの書き換えや削除などを行うことが可能である。そのため、マクロウイルスに感染したドキュメントは、ファイルを開いただけでウイルスが実行され、自己増殖などのウイルス活動が行われるようになる。

今までに大きな被害のあった代表的なコンピュータウイルスとしては、Nimda (ニムダ)^{註58)}、Klez (クレズ)^{註59)}、Bugbear (バグベア)^{註60)}、Badtrans (バッドトランス)、CodeRed (コードレッド)、Sircam (サーカム)、LOVELETTER (ラブレター)、Happytime (ハッピータイム)、MTX (マトリックス)、Melissa (メリッサ)、Laroux (ラルー)、MSBlaster (エムエスプラスター)、SQLSlammer (エスキューエルスラマー)、Mydoom (マイドゥーム)、Netsky (ネットスカイ)、Bagle (バグル)、Sobig (ソービッグ)、Mimail (ミメール)、Antinny (アンティニー)、Swen (スウェン)などを挙げることができる。

1-3 暗号技術の不正的使用^{註61)}

最近、高度情報化社会において情報を保護するための最善の方法として暗号技術が活発に論議されている。また、電子商取引の急増にあわせて各国はプライバシーの保護、国家および産業界の重要情報の保護、知的財産権の保護などのため暗号使用の必要性を認識し、多様な方策を模索・実施中である。

暗号技術は元々国家の秘密を保護する目的で軍事、外交分野で使用し始め、金融機関の電子資金移動（EFT; Electronic Funds Transfer）^{註62)}に広く用いられ、経済、金融分野で確固たる地位をとった以来、同一性の認証（authentication）、暗号化キーに対する管理（key management）、電子署名（digital signature）、身元確認（identity）など広範囲な応用分野の開拓により今日には個人や企業間のネットワークに至るまで普遍的に用いられている。

1-4 電子商取引の安定性侵害

電子商取引におけるセキュリティ攻撃の類型としては次のようなものが挙げられる。まず第一に、盗難（confidentiality 攻撃）である。ネットワークでの重要な情報が第三者に知られる、すなわち電子決済の際にカード番号などの主要情報が第三者に知られ、不正に使用される場合などである。

第二に、改造・変造（integrity 攻撃）である。ネットワークの途中に重要な情報が改造されること、すなわち電子決済の際に口座間の貨幣価値移動を指示する場合、受信口座が改造される場合などである。

第三に、偽装・仮装（authenticity 攻撃）である。顔が見えないネットワークで偽装し情報を送信すること、すなわち電子決済の際に社会的に信用度の高い商店に仮装し、消費者から電子マネーを騙し取る場合などである。

第四に、送受信否認（non repudiation 攻撃）である。電子マネーを受け取りながら受け取らなかったと否認することや、電子決済の際に小売店より商品を受け取ったにもかかわらず、受け取らなかったと否認する場合などである。

2. 一般的サイバー犯罪の類型と手法

一般的サイバー犯罪として、まず第一に、サイバー詐欺が挙げられる。サイバー詐欺による被害類型としては、代金決済後商品が、配達されないケースが最も多く、次に無料利用を仮装した料金の請求、契約撤回の不可能などである。そして、過大な料金請求、サイバー投資詐欺、ID やパスワードの盗用による通信料金被害、クレジットカード情報を盗用した金融被害などである。

第二に、知的財産権侵害^{註63)}が挙げられる。ネットワーク環境の高度化により著作権侵害行為も広域性と迅速性を持ち、個別ウェブサイトのユーザーが急増することで、最近には他人のウェブサイトに掲示された資料をコピーし自分の創作物や所有物に偽装する行為も増加しつつある。これ以外にも超高速大容量インターネット使用環境により可能にした映像物などマルチメディア・コンテンツ・ハッキング（multimedia contents hacking）^{註64)}は著作権問題と併せて世界的な文化戦争時代の最大の難題として浮き彫りにされている。

第三に、サイバー性暴力である。サイバー性暴力とは、サイバー空間で他人に性的羞恥

心や嫌悪感、または不快感を与えうる言語や絵、写真などにより意思表示をする行為、またはこれにより相手に性的羞恥心や嫌悪感などを誘発させる行為のことである。すなわち、サイバー性暴力とはサイバー空間で相手の望まない性を道具として影響力を行使し、相手に被害を与える行為である。このようなサイバー性暴力に含まれるものとしてはサイバー淫乱物の掲示、サイバーストッキングなどが挙げられる。

第四に、サイバー名誉毀損および侮辱が挙げられる。サイバー空間での名誉毀損は急激に増加し、深刻な社会問題となっている。サイバー空間での非対面性と匿名性、そして時空を超越するなどの特性により、他人に対する誹謗や言語暴力は現実の世界とは比較にならないほど頻繁に発生している。サイバー空間での名誉毀損や侮辱は現実世界のこれとは異なり、サイバー空間に名誉毀損の内容を掲載・アップグレードする瞬間、不特定多数がその内容を閲覧することができる点で、その被害の深刻性はきわめて大きいといえる。

しかし、現実的にサイバー空間で名誉を毀損した者を探すことは難しく、名誉毀損の内容を見た不特定多数が他のウェブサイトや掲示板などに広げることもできる点で、現実の世界より名誉毀損の被害者に深刻な悪影響を与えることになる。

第五に、サイバー賭博^{註65)}である。最近、インターネットサイトに開場したサイバー賭博場には、サイバー賭博に中毒した人々が集まり、深刻な社会問題になっている。ここに賭博サイトの詐欺行為およびハッキング行為まで加わり、その副作用が社会全般に拡大されている。しかし、このような被害事例よりもっと大きな問題は、サイバー賭博参加者が、自らの行為が不法行為（犯罪）である事実さえも認識していないことである。すなわち、サイバー賭博は、参加者の年齢、性別、職業などが分からないのみならず、賭博に使用される資金が参加者の資金であるか、または他人のクレジットカードを盗んで使用しているかが分からない状態で行われている。また、サイバー賭博開場者がトリックを使ってもこれを防止する方法がなく、コンピュータのミスで勝者に賭博資金を超過分配したり、勝者がないように誤判する場合にこれを仲裁する人や解決方法がないなど機能的・道徳的弊害が常存している。

V. おわりに—サイバー犯罪への対策—

21世紀、知識・高度情報化社会でのサイバー犯罪への対応策^{註66)}について、サイバー空間の特性を考慮に入れて簡略に述べることで本稿のむすびとしたい。

まず第一に、サイバー犯罪への対応のための法律・制度の体系的整備を挙げることができる。現在、情報化と関連した社会現象は急激に変化し、犯罪現象も既存の法律と制度では効果的に対応できないケースも多く発生している。すなわち、行為の社会的弊害から見るとそれ相当の処罰を受けるべきであるにも拘わらず、処罰法規が整備されておらず処罰できないケースも多く発生している。

したがって、このような問題点に対応できる統合的（総合的）法律の制定が不可欠であろう。すなわち、各種サイバー犯罪に対応できる構成要件を統合し、体系的で一貫性のある法律を制定することが先決であろう。既存の刑法を改正しサイバー犯罪関連条項を挿入したり、既存の関連法律を各々整備するよりは統合法を制定することがより効果的である

といえる。

第二に、人材育成・機材の充実強化^{註67)}を図るべきである。情報通信技術を悪用したサイバー犯罪に適切に対処していくためには、高度な専門知識を備えた人材の育成が必要不可欠である。それらの技術を習得させるために、教育・訓練およびそのための環境の整備を進めることが重要である。また、サイバー犯罪発生 of 未然防止および発生した際の的確な対処活動とそれぞれに資する機材の充実・強化を図るべきである。あわせて、それら機材の高度化、効率化に資する調査・研究を行うことも重要であろう。

第三に、サイバー犯罪の国際性に合わせて、外国の関係機関との連携強化を図るべきである。サイバー犯罪は特定な地域に限定して発生することではなく、国境を超越して発生しているのが現状である。したがって、特定国家の法律のみを一方的に適用することはできず、関連当事国間の緊密な協調体制が必要であろう。

最後に、サイバー犯罪に対する一般国民の認識転換の必要性が挙げられる。今までの一般的な認識として、サイバー空間を利用して行われる犯罪行為に対しては比較的に寛大であったことも事実であろう。すなわち、他のネットワークや他人のコンピュータに自由に出入りし、情報を盗んだり破壊する行為などのサイバー犯罪について、人のまねできない専門知識を持つ人々が好奇心で一回行った行為程度に考えたり、先端技術者であるといった、英雄視する傾向も多かったことも事実であろう。

しかし、サイバー犯罪も既存の犯罪と同様、社会秩序を害する厳然たる犯罪の一つとして認識すべきである。したがって、それに対する処罰も既存の犯罪と同様に行われるべきである。そして、場合によっては一般的な犯罪に対する処罰をより厳重に行い、サイバー犯罪を抑制する必要もあろう。

註)

註1) Choi, J. H. (2001), *A Study on Criminal of Cyber*, KyungSung Univ., pp. 4 - 6 ; カン・ドンボム「サイバー犯罪と刑事法的対策」『刑事政策研究』第11巻第2号, 65~67頁などを参照されたい。

註2) 成耆政「情報通信技術」小林末男監修『現代経営組織辞典』創成社, 2006年2月, 175~176頁。

註3) 成耆政「インターネットショッピングにおける情報技術受容に関する概念的考察」『松本大学研究紀要』第4号, 松本大学, 2006年1月, 51~64頁。

註4) 2000年2月7日, ヤフーコンピュータシステムにハッカーが侵入し, 午前10時30分(現地時刻)から3時間の間サービスが中断されたことで, 約50万ドルの広告損失を被ったことは有名である。

註5) <http://www.buy.com/>

註6) 成耆政「インターネットショッピングモール企業における CRM 戦略の構築」『経営論集』第21巻, 朝日大学経営学会, 2006年9月, 40~43頁を参照されたい。

註7) 成耆政 (2006), 前掲書, 43~45頁を参照されたい。

註8) CNET Networks, Inc. はアメリカを中心に世界12カ国で「CNET」や「CNET News.com」, 「ZDNet」, 「TechRepublic」, 「Builder.com」, 「GameSpot」などのオンラインメディアを運営している。そして150カ国を超える国々から, 情報技術の発展を担う数多くの技術者, 市場関係者, そしてユーザーにアクセスされている CNET Networks のメディアでもある。テクノロジーに関する幅広いジャンルの信頼できる情報源をもとに, ニュース, レビュー, サービスを日々提供し, 各地域のテクノロジーマーケットにかかわる情報を, それぞれの言語で独自に提供するウェブメディアとして, 世界で最も広範にわたる地位を確立している。また「Computer Shopper」などの雑誌発行や, IT 関連のイベント運営などにも携わっている (シーネットネットワークスジャパン株式会社のウェブサイト資料による)。

註9) アメリカ E*TRADE FINANCIAL Corp. は, 当初システム開発会社としてスタートし, 数々のインターネット取引システムを構築し, そのシステムを Fidelity, Charles Schwab, Quick & Reilly といったブローカーに提供していた。1992年に, 自らも証券業務に進出し, インターネット取引サービス開始後わずか3年余りで, 70万口座を超える顧客数を有する全米トップレベルのインターネットブローカーに成

長した。1996年には、ウェブサイト(www.etrade.com)を立ち上げ、現在では、MediaMetrix 社より「全世界で最も訪問者の多い金融サイト」として評価されるまでに至っている。また、サービス開始以来継続して、アメリカの評価企業である Gomez 社よりオンライン証券企業として No. 1 の評価を受けている。2005年12月末現在の口座数は420万以上になっており、アメリカ、日本だけではなく、現在では、オーストラリア、カナダ、デンマーク、ドイツ、韓国、スウェーデン、イギリス、香港、フィンランド、フランス、アイスランドと全世界13カ国でそれぞれの E*TRADE のサービスを展開、インターネットをつうじた24時間取引、商品の多様な品揃え、豊富な情報サービスなど、E*TRADE のサービスはグローバルリーダーとして、日本をはじめ世界各国でサービスを展開している (SBI E*TRADE SECURITIES Co., Ltd のウェブサイト資料による)。

- 註10) DDoS については、第IV節のサイバー犯罪の類型を参照されたい。
- 註11) 「情報セキュリティの現状2000年版」Rev. 1.1, 情報処理振興事業会セキュリティセンター, 26頁。
- 註12) <http://www.pref.toyama.jp/>
- 註13) 1948年ウィーナーが「Cybernetics」という作品を発表した以降、サイバーという用語はインターネットの発達と普及に伴い多様な意味で使われるようになった (Wiener, N<1948>, *Cybernetics; or Control and Communication in the Animal and the Machine*, Kessinger Publishing)。そして、サイバー空間 (Cyberspace) という言葉はギブソン (W. Gibson) の SF 小説, *Neuromancer*<1984, Ace Books>で初めて登場し、ここでギブソンはサイバー空間を合意により成立された幻想と表現し、人間の脳に直接連結されたネットワーク上の仮想空間という意味で使用した。
- 註14) Parker, Donn. B.(1998), *Fighting Computer Crime: A New Framework for Protecting Information*, New York: John Wiley & Sons.
- 註15) Thomas, D. (2000), "Criminality of the Electronic Frontier: Corporality and the Judicial Construction of the Hacker", in Thomas D, & Loader, B. D. (eds.), *Cyber Crime: Law Enforcement, Security and Surveillance in the Information Age*, London: Routledge, pp. 17-35.
- 註16) <http://www.npa.go.jp/cyber/>
- 註17) 1949年に発足し、現在、45カ国が加盟している欧州評議会は、1997年からサイバー犯罪に関する刑事法制について検討し、2001年11月8日に、ストラズブール (署名式典はハンガリーのブダペストで開催) で30カ国の署名によりサイバー犯罪条約を採択した。日本はオブザーバーとして検討に加わってきたが、同年11月23日に同条約に署名した。本条約は、サイバー犯罪に対応しようとしている世界で初めてのもので、前文と4章48カ条で構成され、第1章用語の使用、第2章各国レベルで講じられるべき措置、第3章国際協力、第4章終章である。この分野におけるグローバル・スタンダードとして重要な役割を果たすことになるとみられている本条約は2004年3月30日衆議院、同年4月21日に参議院で承認された (Enjoy Life のお役立ち辞書による)。
- 註18) これについては、石井徹哉「サイバー犯罪条約に関する覚書き」『奈良法学学会雑誌』第15巻1・2号、奈良産業大学、2002年9月、47～58頁；山根信二「コンピュータ専門家のサイバー犯罪条約への取り組み」『法学情報』社団法人電子情報通信学会、2003年10月、13～16頁；「欧州評議会サイバー犯罪条約と我が国の対応について」『サイバー刑事法研究会報告書』経済産業省、2002年4月、1～116頁；陳一・横溝大「サイバーセキュリティと国家管轄権」N T Tデータ技術開発本部システム科学研究所編『サイバーセキュリティの法と政策』N T T出版、2004年3月、64～76頁などを参照されたい。
- 註19) Mark D. Goodman, *Why the police don't care computer crime*.
- 註20) 人見信男「コンピュータ犯罪の発生状況」『警察学論集』立花書房、1982年11月、10頁。
- 註21) Bequai, August(1978), *Computer Crime*, Lexington Books, D. C. Health & Company, p. 4.
- 註22) 安富潔「サイバー犯罪との闘い」『日経デジタルコア活動レポート』2002年8月。
- 註23) コンピュータ不正操作とはコンピュータにより処理、伝達、保存される前段階、すなわちコンピュータシステムを運用する全体の段階でデータを不正に操作する一切の行為を指す。
- 註24) コンピュータスパイとはコンピュータのデータとプログラムなどの情報を権限なしで獲得、またはこれを漏洩する行為を意味する。
- 註25) コンピュータ破壊とはハードウェアとしてのコンピュータの全部、または一部を破壊したり作動しないようにする行為とデータやプログラムを貯蔵するメディアを破壊する行為を指す。
- 註26) コンピュータ無権限使用とは、正当な使用権限を持ってない者が他人のコンピュータを自らのために一定期間作動させる行為のことを指す。
- 註27) Sieber (1986) はコンピュータ犯罪の一般的な類型をその被害法益を基準に、コンピュータ関連経済犯罪 (computer-related economic crime)、プライバシー侵害のような個人的権利、ないし人格的法益に対する犯罪 (computer-related offenses against personal rights)、そして超個人的法益に関する犯罪 (computer-related offenses against super-individual interests) に分類している (Sieber, U.<1986>, *The International Handbook on Computer Crime*, Chichester: John Wiley & Sons, p. 3)。
- 註28) <http://www.htcia.org/>

- 註29) <http://www.HighTechCrimeCops.org/>
- 註30) 趙炳仁「ハイテック犯罪に関する研究」『刑事政策研究』第10巻第3号, 1999年, 191頁。
- 註31) Baik, S. C. (2002), *A Study on Crimes in the Cyberspace-Cybercrime*, Pukyong Univ., pp. 24-25.
- 註32) TCP/IP (Transmission Control Protocol/Internet Protocol) は米国防総省の資金援助によるネットワークプロジェクト DARPA NET (Defense Advanced Research Project Agency Network) で開発されたネットワークプロトコルのことである。1980年代のはじめに UNIX 4.2 BSD で実装されてから急速に普及が進むことになった。Internet の標準プロトコルであり、現在、最も普及しているプロトコルである。ネットワーク層プロトコルは IP で、トランスポート層プロトコルは TCP (Transmission Control Protocol) と UDP (User Datagram) の二つで構成されている。TCP/IP プロトコルに関する規格書や運用技術情報などは、すべて RFC (Request for Comments) という文書にして配布されている (ASCII.jp のデジタル用語辞典のウェブサイト資料による)。
- 註33) この節は、警察庁「平成18年のサイバー犯罪の検挙及び相談状況について」2007年2月；警察庁「警察庁情報セキュリティ政策大系-2004~サイバー犯罪・サイバーテロに立ち向かう警察~」2004年8月などによる。
- 註34) これは、他人の識別符号をどのコンピュータに対する識別符号であるかを明らかにし、またはこれを知っている者の求めに応じ、アクセス管理者や利用権者に無断で第三者に提供する行為のことをいう。
- 註35) フィッシング (phishing) とは、金融機関などからの正規のメールやウェブサイトを装い、暗証番号やクレジットカード番号などを搾取する詐欺のことである。「釣り」を意味する「fishing」が語源であるが、偽装の手法が洗練されている (sophisticated) ことから「phishing」と綴るようになったとする説もある。代表的な手口としては、メールの送信者名を金融機関の窓口などのアドレスにしたメールを無差別に送りつけ、本文には個人情報を入力するよう促す案内文とウェブページへのリンクが載っている。リンクをクリックするとその金融機関の正規のウェブサイトと、個人情報入力用のポップアップウィンドウが表示されるようになり、メインウィンドウに表示されるサイトは「本物」で、ポップアップページは「偽者」である。本物をみて安心したユーザーがポップアップに表示された入力フォームに暗証番号やパスワード、クレジットカード番号などの情報を入力・送信すると、犯人に情報が送信されるようになる (IT 用語辞典 e-Words のウェブサイト資料による)。
- 註36) ワンクリック請求とは、ブラウザなどで表示されている URL を1回クリックするだけで、何を根拠に、何の対価として、どこの誰に払うのかが分からないが、請求が発生する仕組みのことをいう。
- 註37) 買受け捜査とは、身分を隠した捜査員が犯人側 (売り手) に接触する「おとり捜査」の一種で、従来、違法なコピー商品 (海賊品) や偽ブランド品、ポルノ雑誌など偽物密売の取り締まりに用いられてきた捜査手法の一つである (ネット情報局のウェブサイト資料による)。警察庁は2006年10月末にネットの違法品販売にこの買受け捜査を積極的に活用するように指示をしている。
- 註38) この節は、羽室英太郎『サイバー犯罪・サイバーテロの攻撃手法と対策』立花書房, 2007年4月；Park, S. T. (2004), *A Study on the Present Situation of Cyber crime and It's Countermeasure*, Yeungnam Univ. ; Paik, K. H. (2001), *A Study on Cyberterrorism*, KIC などによる。
- 註39) 安保などはサイバー犯罪 (攻撃) の類型を①なりすまし型, ②詐欺型, ③コンピュータ型, そして④攻撃型の4種類に分類している (安保克也・下畑法近『ネットワーク時代のテロリズム-しのび寄る脅威との闘い・サイバーセキュリティ-』三修社, 2003年2月, 80~86頁)。
- 註40) クラッカーとはコンピュータシステムに権限を持たないのにアクセスしようとする人物のことである。これらの人々はしばしばハッカーとは対照的に悪意を持っており、システムに進入する多数の手段を思いのままに使う人である (RFC1983/FYI18 の *Internet User's Glossary*, p.12による)。
- 註41) Levy, S. (2001), *Hackers: Heroes of the Computer Revolution* 10, Penguin USA.
- 註42) ここでは省略するが、ハッキングの技法として buffer overflow, snoofing attack, sniffing attack, spoofing attack (IP spoofing, ARP spoofing, e-mail spoofing, DNS spoofing), smurfing attack, spam mail, herf gun, scan attack, backorrifice, backdoor, wire tapping, data diddling, super zapping, scavenging などを挙げることができる。
- 註43) DoS 攻撃については、羽室英太郎『サイバー犯罪・サイバーテロの攻撃手法と対策』立花書房, 2007年4月, 139~174頁に詳しい。
- 註44) トロイの木馬の一般的な機能としては、パスワードハッキング、ファイルの削除および修正、ファイルのアップロードおよびダウンロード、警告メッセージの送信、システム終了およびブッティング、そしてモニター調整などを挙げることができる。
- 註45) 現在まで登場したトロイの木馬プログラムは100以上で、継続的な機能拡張と GUI の便宜性によりその被害は益々増加する趨勢である。
- 註46) これは、ハッカー集団の「Cult of the Dead Cow」が開発・配布しているクラッキングツールのことである。他人の Windows マシンを乗っ取り、インターネットなどをつうじて、遠隔地からデータの破壊を含むあらゆる操作を自由に行なうことができるようになる。乗っ取りを行なうためのプログラムは

電子メールの添付ファイルの形で送られてくる。ユーザーが誤ってそのファイルを実行すると、乗っ取りプログラムがこっそりシステムの内部にコピーされる。クラッカーは「管理者用」ツールを使って、遠隔地からインターネットなどをつうじて、ユーザーに気づかれることなく、あらゆる操作を行なうことができるようになる（IT用語辞典 e-Word ウェブサイト資料による）。

註47) これは遠隔操作機能を備えた、Windows に感染するトロイの木馬の一つである。目標となるマシンに「NetBus サーバ」を送り込み、クライアントプログラムから目標のマシンを操作することができる。サーバとクライアントのやり取りには TCP/IP が使われており、「12345」「12346」「20034」のいずれかのポートを利用するので、これらのポートの利用状況から検出することも可能である。現在ではパソコンの遠隔管理用にシェアウェアとして販売されているが、クラッキングツールとして悪用されていた過去があるため、イメージは回復していない。今でもほとんどのアンチウイルスソフトが NetBus を外部からの侵入として検出している（IT用語辞典 e-Words のウェブサイト資料による）。

註48) Deep Throat は、悪名高い Back Orifice や NetBus ツールと同様のハッカーが使用するリモート管理ツールである。ハッカーは Deep Throat を使ってリモートシステム上のデータにアクセスし、いくつかの Windows 機能の制御を奪うことができる。Deep Throat ツールは、クライアント部とサーバ部から構成され、サーバ部はアクセス先のリモートシステムにインストールされる。特別なドロップパーを使って無作為な名前で TEMP ディレクトリにサーバ部が挿入されることもある。実行されると、サーバ部は自分自身を Windows ディレクトリにインストールし、これにより、Window の次回起動時に自動的に実行されるようになる（日本エフ・セキュア株式会社のウェブサイト資料による）。

註49) SubSeven バックドアは、1999年5月に初めて発見され、最初のサンプルは、バックされておらず容易に検出できた。後のバージョンでは、バックされたため Win32 'Aspack' 互換伸張機能を持たない最新のアンチウイルス製品では、検出が困難な状況である。このバックドアは、ニュースグループや E メールで異なった名前として配信されている。起動するとこのバックドアは、自分自身のファイルを¥Windows¥ディレクトリにコピーし以下のファイルと置き換える。SERVER.EXE, KERNEL16.DLL, RUNDLL16.COM, SYSTEMTRAYICON!.EXE または WINDOW.EXE（ファイル名は、バージョンごとに異なる）さらに、WATCHING.DLL ファイルを¥Windows¥System¥に解凍する（一部のバージョンでは、行われない）。その後、バックドアは、次のブート時にメインアプリケーションを起動するためにレジストリに変更を加え、最終的に、その他のレジストリを作成・変更する。このバックドアは、WIN.INI または、System.ini に変更を加えることで自分自身をシステムにインストールすることもできる（日本エフ・セキュア株式会社のウェブサイト資料による）。

註50) これは1999年6月に猛威を振ったコンピュータウイルスである。電子メールを媒介にして、Windows が動作しているコンピュータに感染する。システムに潜入して悪さを働く「トロイの木馬」の機能と、ネットワークをつうじて自己増殖する「インターネットワーム」の機能の両方を兼ね備えたウイルスである。メールに添付された「PrettyPark.EXE」というファイルを開くと感染し、アドレス帳に記載されたアドレスに30秒おきに自分の複製を送信する。また、ユーザーが気づかぬうちにチャットシステムの I R C を使って特定のサーバへ接続し、ウイルスの作者がそのコンピュータを監視したり操作したりできるようにしてしまう（IT用語辞典 e-Words のウェブサイト資料による）。

註51) これは旧通商産業省制定（1995年7月7日、告示第429号）の「コンピュータウイルス対策基準」の用語の定義によるものである。

註52) 「インターネットと情報セキュリティの基本知識－ウイルスって何?」『国民のための情報セキュリティサイト』総務省のウェブサイト資料より引用した。

註53) <http://www.javascript.com/>

註54) これは Microsoft 社によって開発されたスクリプト言語（簡易プログラミング言語）のことである。同社のウェブブラウザである Internet Explorer 上で動作する。同社のプログラミング言語 Visual Basic のサブセット（簡易版）になっており、さまざまな制限が加えられている。同社のウェブサーバである IIS 上で動作させることもでき、サーバ上でスクリプトを実行して動的に HTML 文書生成する ASP の標準スクリプト言語になっている。また、WSH を利用して、Windows 95/98 や Windows NT/2000 などの環境で、従来より強力なバッチ処理を行なうこともできる（IT用語辞典 e-Words のウェブサイト資料による）。

註55) これは Microsoft 社によって開発されたソフトウェアの部品化技術のことである。従来、OLE コントロールと呼ばれていた技術に、インターネットに対応するための拡張を施したものである。ActiveX コントロールはインターネットやイントラネットをつうじてウェブサーバからダウンロードされ、同社のウェブブラウザである Internet Explorer に機能を追加する形で使用される（IT用語辞典 e-Word ウェブサイト資料による）。

註56) <http://www.java.com/>

註57) Visual Basic for Applications（ビジュアルベーシック・フォー・アプリケーションズ、VBA）は、マイクロソフト社製の Microsoft Office シリーズに搭載されているプログラミング言語である。VBA を使用

することで、Excel や Access などを使用した定型業務を自動化することができる。また、ユーザー独自のフォームを作成することができ、様々なプラグイン (plug-in) を組み込むことでアプリケーションの機能をカスタマイズすることなども可能である (フリー百科事典『ウィキペディア (Wikipedia)』のウェブサイト資料による)。

註58) これは2001年9月にインターネット上で猛威を振るい、それまでで最悪と言われるほど大きな被害を出したコンピュータウイルスの一種である。Microsoft 社の Windows シリーズの OS を搭載したコンピュータに感染する。同社の複数のソフトウェアを介して様々な手段で感染するよう設計されており、初の本格的な複合型ワームとして注目された。Nimda は公開されているウェブサイトの HTML ファイルに JavaScript によるスクリプトと実行可能形式のプログラムとして潜入し、同社の Internet Explorer を介して閲覧者のコンピュータに感染したり、Internet Information Server のセキュリティホールを突いて不正な HTTP リクエストの形で侵入したり、電子メールの添付ファイルに潜んで Outlook Express を介して感染したり、LAN 上でファイル共有機能をつうじて自身の複製を作成するなど、多様な手段で感染する (IT 用語辞典 e-Words のウェブサイト資料による)。

註59) これは2002年春から夏ごろにかけて流行した、Windows に感染するワームの一種である。電子メールや LAN (ファイル共有) を介して伝染する。Klez には亜種が何種類か確認されているが、手口はほぼ同じである。また、Klez は実行可能形式ファイルにも感染する (ファイルに感染した場合は「Elkern」という呼び名に変わる)。Nimda 以降のワームがよく使う手口として知られる、Outlook Express のセキュリティホールを使用して、メールをプレビューしただけでコンピュータに感染する機能も持っている。Klez に感染したコンピュータは無作為に大量のメールを送信するほか、奇数月の6日にはコンピュータ上のデータファイルを削除する破壊活動も行なう。また、一部の亜種はコンピュータ上のデータファイルを添付したメールを無作為に送信するため、機密情報が漏洩する危険もある (IT 用語辞典 e-Words のウェブサイト資料による)。

註60) これは2002年秋に流行した、Windows に感染するワームの一種で、Microsoft 社のメールソフトである Outlook Express の脆弱性を利用して、メールの添付ファイルやネットワーク上のファイル共有を介して感染する。BugBear はトロイの木馬型ワームで、Outlook Express でウイルスを含んだメールの本文を表示させただけで感染プログラムが実行される。感染すると、Outlook Express の送受信トレイや、メールボックスと類推される拡張子のファイルをディスク内から探し出し、その中に含まれるメールアドレスを収集し、自分自身のコピーをメールの添付ファイルとしてユーザーに気づかれないようこっそり送付する (IT 用語辞典 e-Words のウェブサイト資料による)。

註61) Park, S. T. (2004), *A Study on the Present Situation of Cyber crime and Its Countermeasure*, Yeungnam Univ., p. 21.

註62) EFT (electronic funds transfer system) は電子口座決済、電子資金振り替えシステムのことで、コンピュータとデータ通信によって、預金口座間の資金移動や決済を処理するシステムのことである (キャッシング・クレジット・金融用語ガイドのウェブサイトによる)。

註63) Choi, J. H. (2001), *A Study on Criminal of Cyber*, Kyungsung Univ., p. 27.

註64) これは映画館でデジタルカメラにより映画を録画した後、インターネットに流すなどの犯罪のことをいう。

註65) Choi, J. H. (2001), *ibid*, p. 32.

註66) 日本 IBM は日本企業150社を含む、世界17カ国 (日本、アルゼンチン、オーストラリア、ブラジル、カナダ、中国、チェコ、フランス、ドイツ、インド、イタリア、メキシコ、ポーランド、ロシア、スペイン、イギリス、米国) の企業3,002社に対して企業のセキュリティーに関する調査 (2005年12月から2006年1月) を実施した。その結果によると、組織的なサイバー犯罪への十分な防護対策を取っていると確信していると回答した企業は、世界全体が59%に対し、日本は15%にすぎないことがわかった (japan.internet.com のウェブサイト資料による)。

註67) ここで取り上げている「人材育成・機材の充実強化」についてはすでに実施されている対策である。詳しくは、警察庁「警察庁情報セキュリティ政策大系-2004~サイバー犯罪・サイバーテロに立ち向かう警察~」2004年8月、22~23頁を参照されたい。

参考・引用文献

1. NTT データ技術開発本部システム科学研究所編『サイバーセキュリティの法と政策』NTT 出版, 2004年3月。
2. 安保克也・下畑法近『ネットワーク時代のテロリズム』三修社, 2003年2月。
3. 藤原宏高『サイバースペースと法規制』日本経済新聞社, 1997年10月。
4. 羽室英太郎『サイバー犯罪・サイバーテロの攻撃手法と対策』立花書房, 2007年4月。
5. 安保克也・下畑法近『ネットワーク時代のテロリズムーしのび寄る脅威との闘い・サイバーセキュリティー』三修社, 2003年2月。

6. 江畑謙介『情報テロ—サイバースペースという戦場—』日経 BP 社, 1998年 5 月。
7. H & C クラブ『ハッキング防衛マニュアル—ハッキング・手口知る人達の「本当の」ディフェンスガイド—』データハウス, 1999年 7 月。
8. プチワラドットコム『ハッキングのわざが手に取るようにわかる本』秀和システム, 2001年12月。
9. back section『Windows のハッキングマニュアル』データハウス, 1999年 9 月。
10. プチワラドットコム『ハッキングする？ハッキングされない？』ラトルズ, 2002年11月。
11. Angelis, G. D. (1999), *Cyber Crimes*, Philadelphia : Chelsea House Publishers.
12. Clifford, R. D. (ed.)(2001), *Cyber Crime : The Investigation, Prosecution and Defense of a Computer-Related Crime*, Durhan : Carolina Academic Press.
13. Parker, D. B.(1998), *Fighting Computer Crime : A New Framework for Protecting Information*, New York : John Wiley & Sons.
14. Sieber, U. (1986), *The International Handbook on Computer Crime*, Chichester : John Wiley & Sons.
15. Taylor, P. (2000), “Hackers : Cyberpunks or Microserf ?”, in Thomas D. & Loader, B. D. (eds.), *Cyber Crime : Law Enforcement, Security and Surveillance in the Information Age*, London : Routledge, pp. 36-55.
16. Thomas, D.(2000), “Criminality of the Electronic Frontier : Corporality and the Judicial Construction of the Hacker”, in Thomas D. & Loader, B. D. (eds.), *Cyber Crime : Law Enforcement, Security and Surveillance in the Information Age*, London : Routledge, pp. 17-35.