成蹊大学理工学研究報告
J. Fac. Sci. Tech., Seikei Univ.
Vol.47 No. 1 (2010) pp.93-104
（研究報告）

情報通信（ICT）技術の進展と法律問題（その３）
―ハイテク犯罪：サイバーテロ，違法・有害情報問題―

村上　仁己[*1]，尾形　哲志[*2]，樋口　政和[*3]，川崎　秀二[*4]

Development of Information and Communication Technologies and Its Impact to Legal Issue (3)
― Technological crime：Cyber-attack and illegal and harmful information ―

Hitomi MURAKAMI[*1], Satoshi OGATA[*2], Masakazu HIGUCHI[*3], Shuji KAWASAKI[*4]

ABSTRACT：Development of Information and Communication Technologies (ICT) and their penetration by Internet and mobile phone have given deep impact on our daily lives. Our previous papers already published introduced and discussed such ICT impacts on fusion of communication and broadcasting, copyright and privacy problems as well as personal information protection. Recently, there happened serious troubles in network society by cyber attack from China to Google and from Korea to `2-channeru` which is the biggest Bulletin Board System (BBS) in the world. Taking into account such events, present paper discusses technological crime, such as cyber-attack and harmful information.

Keywords：Internet, mobile phone, cyber-attack, bulletin board system, content filtering

（Received March 25, 2010）

１．はじめに

本論ではこれまで，情報通信技術と，その制度あるいは規制の枠組としての法制度との関連を主題とし，技術の進展によって侵害される可能性のある既存の諸権利と技術革新のもたらす有用性との関連を論じ，具体的な例題として，放送と通信の枠組みの見直し問題，著作権を巡る問題，あるいは個人のプライバシー問題を取り上げた[1),2)]。

既に前２回[1),2)]の論述で検証されたことは，技術の進歩は当該技術が係わる分野の変革をもたらすだけでなく，時として社会の秩序や一般的な意識をも変革させる働きをすることがあることであった。また，その技術の社会的な有用性や合理性が実証（ある場合は否定）されるには相応の時間がかかり，それが一般的な合意形成となるには更なる時間が必要になることでもあった。そしてその一方で，法制度は多く，既存の制度や仕組み，秩序を維持する様作用する。これは「法」というものの基本的な性格であり，また役割に起因するところではあるが，これが技術進歩を矯める要素であったこと――などである。

これらの観点から，本論は，その主基調として，「法制度は技術進歩を矯める働きをすべきではなく，それが諸権利との調整においてやむを得ない場合であっても，規制は必要最小限度でなくてはならない」ことを主張してきた。

本稿で今回取り上げるのは「ハイテク犯罪」である。前述した，これまでの本論の主基調は今回に関しては当てはまらないが，「ICT 技術の進展と法律問題」を論じるには，避けて通れない問題として取り上げる。

いわゆるハイテク犯罪（最近，官庁などを中心に「サイバー犯罪」という言葉が使われている例が多いため，本稿でも以降では一連の犯罪を「サイバー犯罪」と呼ぶことにする）と呼ばれる情報技術に関連（あるいは情報

[*1]：情報科学科教授 (hi-murakami@st.seikei.ac.jp)
[*2]：コア・マネージメント（株）代表取締役
[*3]：情報科学科ユビキタス研究室研究員
[*4]：情報科学科ユビキタス研究室客員研究員

技術を利用）した犯罪は，非常に多岐にわたるが，大きく二つのジャンルに分けられる。

一つはコンピュータ及びネットワーク（仮に「システム」と呼ぶ）を標的とするものであり，コンピュータウィルスやサイバーテロなどの直接的なシステムに対する攻撃，不正アクセスなどが挙げられる。他の一つは，ネットワーク（システム）を利用する犯罪群で，オークション利用に代表される詐欺行為，児童ポルノ・売春や出会い系サイトなどの違法・有害情報，迷惑メールまた悪質商法，著作権侵害の違法コピーの販売，さらには名誉毀損や誹謗中傷による加害などがある。

これらの犯罪は，ICT 技術の進歩とそれに伴うネットワークの拡充による利便性という「光」の部分の登場によって生み出された「影」の部分である。それ故に，サイバー犯罪は，これまでの多くの犯罪行為と異なる特徴を持っている。その一つは，ネットワークの有意性である性格そのままに，犯罪の遂行や被害の拡大が即時（速効）性を持ち，地域，場合によっては国を超えた国際的な拡がりをもつ，まさにユビキタスの「何時でも，何処でも」の犯罪といえる点である。そして，サイバーテロやウィルスなどの犯罪は，被害者にとっては重大な損失を与える一方で，加害者である犯罪者にとっての利得や意図（通常は動機という）は必ずしも明確でない場合も多く（政治的意図を持つ大規模なテロもあるが），加えて匿名性が高く，犯罪の痕跡も残りにくいという，従来にはない犯罪の形がそこにある。

このような加害者＝犯罪者と被害者の存在，またその因果関係を前提とするこれまでの法律の体系とは異なる犯罪に対して，法が規制するべきは何なのか，また処罰するべき対象（犯罪）はどのような事象なのか，技術的側面からはどのような対処が必要また可能なのか，個々の犯罪事象毎に対応法とともに検証する。

２．サイバー犯罪の実態

つい最近，警察庁が昨年 1 年間（平成 21 年中）のサイバー犯罪の検挙状況についての集計を公表した [3]。この公表資料によれば，平成 21 年中のサイバー犯罪(情報技術を利用する犯罪)の検挙件数は 6,690 件で前年より 369 件(5.8%)の増加であった。統計を取り始めた平成 17 年からの過去 5 年間で約 2 倍に増加し，過去最多となっている。

内訳を見ると，コンピュータ等システムを対象とする直接的な事犯が 195 件で前年より 52 件(21.1%)減少する一方で，不正アクセス禁止法違反は 2,534 件で前年より 794 件(45.6%)増加しており，これは平成 12 年の不正アクセス禁止法施行後，最多となっている。これに対し，ネットワークを利用した犯罪では，ネットワーク利用詐欺，青少年育成条例違反，出会い系サイト規制法違反が減少する一方で，わいせつ物頒布，児童ポルノ事犯が増加しているが，利用犯罪全体では前年比 1 割弱の減少となっている（図 1）。

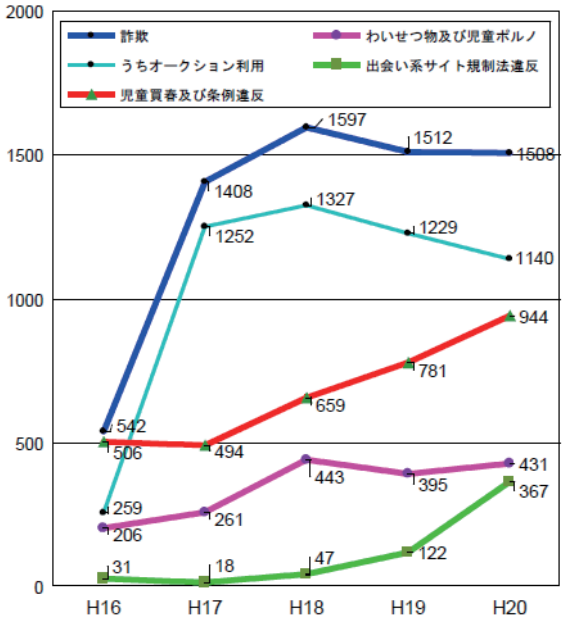

図１　ネットワーク利用犯罪の内訳

公表された数字を多いとするか否かは各様の見方があろうが，注意しなければならないのは，この公表された数字は，事件として立件され且つ容疑者が検挙された数字ということである。話題を集め国際紛争の種ともなっている，中国によるグーグルへのサイバー攻撃（グーグル側の主張と中国当局の事実関係の認識は 180 度異なっており，事実関係は未だ不詳）や最近の韓国からの日本の世界最大のブログである‘２ちゃんねる’へのサイバー攻撃（この事案は，２ちゃんねるのサーバが米国に設置されていたことにより，結果として米国へのサイバー攻撃にもなった）に見られるように，サイバー攻撃（テロ）などネットワークに対する事犯は表面化してもなお犯罪行為の実態，あるいは不法行為を起こした者が不詳の場合が多く，検挙数の統計は実態に比べ，まさに氷山の一角であることは想像に難くない。

３．サイバー犯罪と法律

3．1　法律制定の流れ

サイバー犯罪に対する法律はどうなっているのであろ

うか。わが国においてのコンピュータ関連犯罪に対応するための法整備としては，昭和 62 年（1987 年）の刑法改正によるものが最初である。同年 5 月に可決成立した「刑法等の一部を改正する法律」では，①電子情報処理組織において用いられる電磁的記録について，その不正作出及び供用並びに毀棄を処罰すること②電子情報処理組織による大量迅速な情報処理によって行なわれる業務を妨害する行為を処罰すること③債権・債務の決済等が電磁的記録を用いて自動的に行なわれる事務処理の形態を利用して財産上の不法の利益を得る行為を処罰すること－－等を旨とする改正が行なわれ，新たに，電磁的記録不正作出罪，電子計算機損壊等業務妨害罪，電子計算機使用詐欺罪，電磁的記録毀棄罪などの罪状が設けられた。コンピュータ関連の犯罪（不正）行為に法律が初めて対応し，刑法犯罪としたわけではあるが，この改正は，上記主旨から判るように，それまで刑法がその対象とする犯罪行為にコンピュータが使われることによって付加された行為を取り上げたもので，情報処理システムを対象とする犯罪行為を主眼に規制する法改正とはなっていなかった。

本論で取り上げる，不正アクセスなどのサイバー犯罪の多くは，この時点では未だ法律上の犯罪とはされておらず，サイバー犯罪に対する法対応は，平成 11 年の「不正アクセス行為の禁止等に関する法律」の成立を待つことになる。

3. 2　サイバー犯罪条約

平成 13 年 11 月，フランスのストラスブールで「サイバー犯罪に関する条約」が採択された。わが国もこの条約の起草委員国として参加，署名をし，平成 16 年 4 月の国会承認（批准）を得て，同年 7 月その効力が発生した。

このサイバー犯罪条約は，欧州評議会（Council of Europe）で策定された国際条約で，欧州評議会加盟各国の他，アメリカ，カナダ，オーストラリア，南アフリカ等の参加で策定された。

条約は，サイバー犯罪からの社会の保護を目的とする国際的な法的枠組みを定めるものであり，サイバー犯罪の深化・蔓延に効果的かつ迅速に対処するために国際協力を行い，共通の刑事政策を採択することを目指した。具体的には，コンピュータ・システムへの不正なアクセス，不正な傍受等一定の行為を犯罪とすることを締約国に義務づけた上で，これらの一定の犯罪についての裁判権の設定，これらの一定の犯罪及びコンピュータ・システムという手段によって行われる他の犯罪についての犯罪人引き渡し並びに捜査，訴追及び司法手続における法律上の援助等について規定している。

この条約は，国際条約として発効しながら，各国の利害，国内状況から未だ多くの国で批准されておらず，国際条約としてはその存在自体に疑問を呈する向きもある。条約としては未完であるとの議論，各国の批准が進まない理由など，条約の実効性等の議論はひとまず置き，ここでは条約を，国際化するサイバー犯罪に対する諸外国の共通認識，またその取り組みの方向性を示すテキストと考え，その内容の概略を紹介する。

サイバー犯罪条約は，4 つの章，48 の条文で構成されており，第 1 章ではサイバー犯罪に関する基本用語を定義。第 2 章では，刑事実体法として「不正アクセス」「不正傍受」「データ妨害」「システム妨害」「装置濫用」「コンピュータ関連偽造」「コンピュータ関連詐欺」「児童ポルノ関連犯罪」「著作権及び関連諸権利の侵害に関連する犯罪」をサイバー犯罪として定義し，各犯罪の構成要件を規定するとともに，コンピュータ・データの応急保全や部分開示，捜索・押収，通信記録（トラフィック・データ）のリアルタイム収集や通信内容の傍受などに関する手続法を定めている。第 3 章は第 2 章で定義したサイバー犯罪についての相互援助および引渡し命令を含む国際協力について規定し，第 4 章では最終条項として欧州評議会条約の標準規定について述べている。

この第 2 章で列挙される各種の犯罪が，いわゆる国際的な共通認識としてのサイバー犯罪であり，先の二つの犯罪類型に分ければ，「不正アクセス」「不正傍受」「データ妨害」「システム妨害」「装置濫用」までがシステムを標的とした犯罪であり，「コンピュータ関連偽造」「コンピュータ関連詐欺」「児童ポルノ関連犯罪」「著作権及び関連諸権利の侵害に関連する犯罪」が，システムを利用した犯罪ということになる[4]。

3. 3　関連する現行法規

現在，サイバー犯罪に対処する法律にはどんなものがあるのか，各論で取り上げる「不正アクセス防止法」および「青少年ネット規制法」等青少年保護法令は別として，関連する特別法の概要を簡単に紹介しておく。

3. 3. 1　特定電子メールの送信適正化法（迷惑メール防止法）[5]

正式名称は「特定電子メールの送信の適正化等に関する法律」。平成 14 年 4 月に成立した法律で，その内容は，不特定多数を対象にして一時に送信される広告や宣伝メールを「特定電子メール」として規制するものである。

法律では，一般的に「迷惑メール」と呼ばれるメールを「特定電子メール」と呼称，「営利団体や個人事業者が

自己又は他人の営業につき広告又は宣伝を行うための手段として送信するメール」（法 2 条 2 号）と定義する。

この法律で注目されるのは，対象とする電子メールを，内容からの判断ではなく通信方式を特定することで定義付けをしている点である。すなわち，「その全部又は一部においてシンプルメールトランスファープロトコルが用いられる通信方式」 また「携帯して使用する通信端末機器に，電話番号を送受信のために用いて通信文その他の情報を伝達する通信方式」と同法施行規則で定めている。また，このような「特定電子メール（＝迷惑メール）」を防止する方策としては，送信者の氏名や，受信拒否を可能にするために送信者のアドレスの明示などを送信者に義務付けている。

法律は，平成 17 年と 20 年に改正が行われ，17 年の改正では，送信者を偽装した広告等のメール（スパムなど）について刑事罰が科せられることになった。現行法である平成 20 年の改正では，それまでの広告宣伝メールのオプトアウト方式をオプトイン方式に代えることを規定した。この改正により，広告・宣伝・勧誘等を目的とした電子メールを送信するには，事前に受信者の許可を得ることが必要要件となった。

尚，行政指導等の措置に加えて，違反者には 1 年以下の懲役や 3000 万円以下の罰金が定められている。

3. 3. 2　プロバイダ責任法

通称プロバイダ責任法の正式名称は，「特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律」で，平成 13 年に成立，翌 14 年 5 月に施行された [6]。この法律は，インターネット上で名誉毀損や著作権侵害などの損害賠償が求められる問題が生じた際の「プロバイダ」等（この場合のプロバイダとは，インターネットサービスプロバイダだけでなく，電子掲示板の管理者などを含む＝法律では「特定電気通信役務提供者」）に，損害賠償責任の制限及び発信者情報の開示を請求する権利を定めている。その一方で，権利侵害をされた者に対しては，当該プロバイダに対して発信者情報の開示を請求する権利を認めている。

さらに，プロバイダは，自らの運営するインターネットサービスにおいて，法律や既定の諸権利を侵害（ないしは抵触する）する書き込みがあり，書き込みを行った者の情報が得られない場合に，被害者の依頼により，その書き込みを適宜削除したり非公開に出来る権利や，その管理責任を問われる範囲などが規定された。

3. 3. 3　携帯電話不正利用防止法

正式名称「「携帯音声通信事業者による契約者等の本人確認等及び携帯音声通信役務の不正な利用の防止に関する法律」である [7]。平成 17 年に成立した。犯罪など不正に携帯電話が利用されることの防止を目的とした法律で，携帯電話事業者や携帯電話のレンタル事業者に契約者の本人確認を求めるなど携帯電話の不正使用の防止を図るため作られた。

この法律は，平成 20 年に，多発する「振り込め詐欺」に携帯電話が悪用されている実態から，不正利用規制を強化した改正法が施行されている。

4．サイバー犯罪・各論

サイバー犯罪は，既述の「犯罪条約」の中でも見られたように，非常に多岐にわたっているが，それらの全てを検証することは紙数の関係から出来ない。ここからはそれらの中から各論として「不正アクセス」と「サイバーテロ」，そして青少年保護の問題を含めたいわゆる「有害情報規制」の問題を採り上げていくことにする。

4. 1　不正アクセス（システムに対する犯罪・その 1）

不正アクセスの問題を各論として採り上げるのは，既述の「サイバー犯罪の検挙状況（警察庁）」で述べたように事犯の件数が最も多く（不正アクセス禁止法違反の検挙数は全体の約 4 割），且つここ数年，急速に事犯が増加（前年比 45%増）し，今やサイバー犯罪の中心的存在になっているという事情による。

4. 1. 1　不正アクセスとは

不正アクセスはどのようなものか。一般的に『不正アクセスとは，あるコンピュータへの正規のアクセス権を持たない人が，ソフトウェアの不具合などを悪用してアクセス権を取得し，不正にコンピュータを利用する，あるいは試みること』と定義される。

そして不正アクセスの方法として，①コンピュータの脆弱性を悪用してアクセスする「セキュリティ・ホール攻撃型」②何らかの方法で他人のパスワードを入手し，そのユーザになりすましてアクセスする「識別符号窃用型」の 2 形態に分けることができるとされる。

4. 1. 2　不正アクセスの類型別事案数と犯行の手口（公安委員会資料から）

かつては，上記①のセキュリティ・ホール攻撃型が，不正アクセスの代表的形態であったが，現在では②の「識別符号窃用型」が圧倒的多数となっている。昨年一年間の検挙件数を公安委員会公表資料 [8] から拾うと，②の「識別符号窃用型」による不正アクセスが全体検挙数の 99%（2532 件中の 2529 件）となっている。（同資料での「セキュリティ・ホール攻撃型」は 3 件）。

さらに，上記「識別符号窃用型」2529 件を犯行の手口で見ると，そのほとんどが「フィッシングサイトからの入手(＝2084 件)」によるもので，残りは「共犯者からの入手」「他人からの購入」であった。フィッシングによるパスワードなどの不正入手が最初に確認されたのは平成 17 年であったが（平成 20 年は 88 件），それが昨年（平成 21 年）には 2 千件を超える急増ぶりを示している。

4. 1. 3　不正アクセスから起こされる犯罪（同上資料から）

不正アクセス自体が犯罪であるが，実態的な被害を伴う犯罪は，不正アクセスによって入手された識別符号を使用して行われる。不正に入手されたパスワードなどにより利用されたネット・サービスを見ると，「インターネット・オークション」が最も多く 2147 件，次いで，「電子メール」が 167 件，「オンラインゲーム」が 88 件，「インターネットバンキング」が 83 件－－などであった。

この検挙数字を見る限り，オークション詐欺やゲームでの不正操作が数字的には圧倒的多数を占めてはいるが，これはあくまでも検挙数である。捜査当局に対しては失礼な言いようにはなるが，これらの多くは素人の起こす犯罪である。話題になり，被害の社会的な影響も大きいと思われる「ネットバンキングにおける不正出金」や「偽造カードの不正使用」は，高度な知識・技術を持つプロの犯罪集団による犯罪であり，検挙数が少なくなるのは，これまた当然のことになり，その実態はこの公表データには顕れてこないのではないかと推定される。

4. 1. 4　不正アクセス禁止法

正式名称「不正アクセス行為の禁止等に関する法律」[9]は，これまでみた一連のサイバー犯罪に対処するための法律の中では，最初に作られた法律で，平成11年に公布され，翌12年から施行されている。

この法律を見ていくに先立って，この法律の主旨をまず明らかにする必要がある。法律の名称から，この法律は，不正アクセスに係わる犯罪を処罰するための法律と解するのが一般的であろうが，法律がその目的とするところは，これとは異なる。

重要なポイントなので，少し長く判りにくい文章ではあるが，法律第一条の「目的」をそのまま引用する。『不正アクセス行為を禁止するとともに，これについての罰則及びその再発防止のため不正アクセス行為を受けたアクセス管理者に対する都道府県公安委員会による援助措置等を定めることにより，電気通信回線を通じて行われる電子計算機に係る犯罪の防止及びアクセス制御機能により実現される電気通信に関する秩序の維持を図り，もって高度情報通信社会の健全な発展に寄与すること』(法一条)，である。

この法第一条から見る限り，この法律の目的は，「アクセス制御機能により実現される電気通信の秩序の維持」にある。すなわち，法律において保護するものは「電気通信の秩序」であり，不正に入手される，あるいはされた「情報」ではないことに留意する必要がある。

法は，①不正アクセス行為等の禁止・処罰という行為者に対する規制と②不正アクセス行為を受ける立場にあるアクセス管理者に防御措置を求め，アクセス管理者がその防御措置を的確に講じられるよう行政が援助するという防御側の対策という２つの側面から，不正アクセス行為の防止を図ろうとする（図 2)。

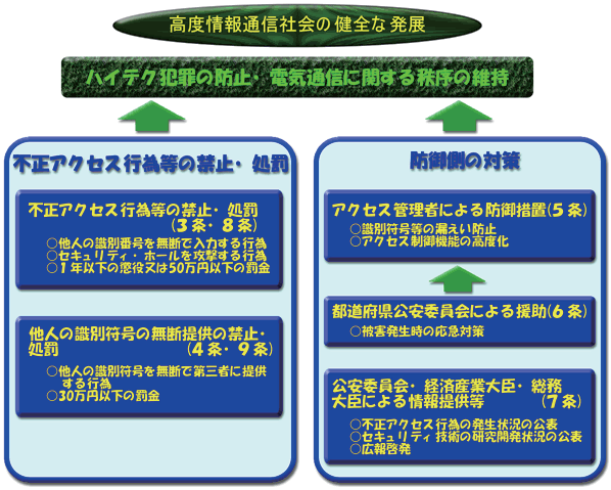

図 2　不正アクセス禁止法の基本構成

そして，「不正アクセス行為」を法 3 条 2 項で以下のように定義する。

① 電気通信回線（インターネット・LAN 等）を通じて，アクセス制御機能を持つ電子計算機にアクセスし，他人の識別符号（パスワード・生体認証など）を入力し，アクセス制御機能（認証機能）を作動させて，本来制限されている機能を利用可能な状態にする行為（1 号）

② 電気通信回線を通じて，アクセス制御機能を持つ電子計算機にアクセスし，識別符号以外の情報や指令を入力し，アクセス制御機能を作動させて，本来制限されている機能を利用可能な状態にする行為（2 号）

③ 電気通信回線を通じて，アクセス制御機能を持つ他の電子計算機により制限されている電子計算機にアクセスし，識別符号以外の情報や指令を入力し，アクセス制御機能を作動させて，本来制限されている機能を利用可能な状態にする行為（3 号）

上記の定義を判りやすく解説すると，①は他人の ID

やパスワードを利用してネットを利用すること（なりすまし）（図 3）②はセキュリティ上の脆弱性（セキュリティホール）やウィルスを使ってのアクセス（図 4）③は認証サーバがある場合を想定しての定義である。

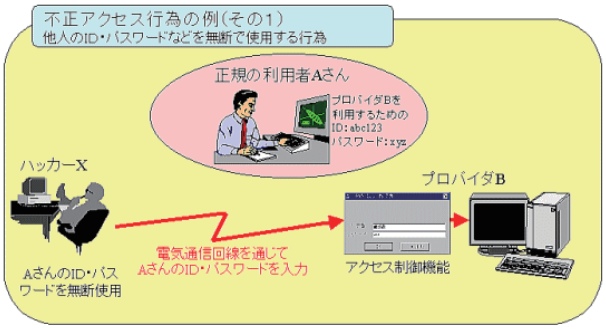

図 3　不正アクセス例（その 1：不正アクセス行為の禁止等に関する法律の概要（警察庁より）

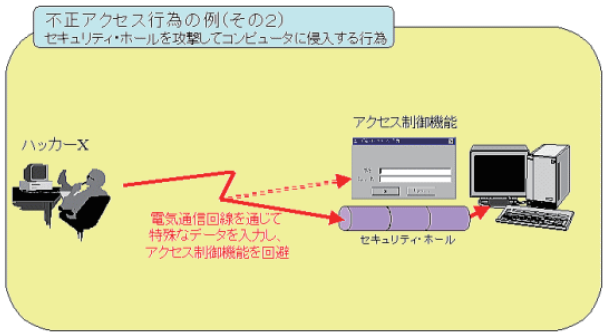

図 4　不正アクセス例（その 2：不正アクセス行為の禁止等に関する法律の概要（警察庁より）

これらの定義を見て判るように，法律が対象としているのは，あくまでもネットワークを通じての行為，またアクセス制御機能を回避また無力化する行為である。従って，他人のパソコンなどの機器に直接的方法（キーボード等で），他人のパスワードを使って入力や出力を行う行為，また，この方法によるデータの不正入手や改竄の行為は，この法律の処罰対象とはなっていない。

不正アクセス禁止法は，ネットワーク秩序の維持・管理を目的とした法律であるため，ネットワークを通じて行為のみを対象としており，全てのサイバー犯罪を対象とするものではないが，サイバー犯罪が脅威とされるのは，既に述べたようにネットワークを介することによる即時性と拡がりであることから，サイバー犯罪対策法の中心的な位置を占める法律といえよう。

4. 1. 5　不正アクセスへの対策（技術的側面を踏まえて）

不正アクセスによる犯罪への予防的な対処の基本は，法律でいうところの識別符号，すなわちユーザ ID やパスワードの適切な管理である。フィッシングに対する注意また適切な対応は勿論必要であるが，これで全てが防げるわけではない。

OS やソフトウェアのセキュリティホールを無くすことも必要な対応である。OS やソフトウェアのアップデートという仕組みは，そのかなりの部分がセキュリティ対策である。米マイクロソフトによれば[10]，Word や Excel などのマイクロソフト Office の文書ファイルを経由して感染するウィルス（ワームなどの不正プログラムを含む）を分析したところ，その 9 割以上が 2 年以上前のアップデートによって修正済みの脆弱性を悪用する手口だったという。利用者がアップデートに対応していないため起きた感染ということになるが，これらウィルスはその利用者にのみ損害を与える場合だけでなくネットを通じて拡散していくことも多い。

ソフトウェアの作成者・販売者が，自らの責任において，アップデートを自動かつ強制的に行える仕組みが必要とも考えられるのではないだろうか。

4. 1. 6　不正アクセス制御手法[11]

不正アクセスのための侵入行為は，一般的に，①事前調査（ポートスキャン，アカウント名の調査等），②権限取得（パスワード，様々な攻撃，特権ユーザ獲得等），③不正実行（ファイル奪取，資源利用，不正プログラム埋め込み，踏み台等），④後処理（裏口作成，証拠隠滅等），という 4 段階のプロセスをとる。このことは，多くのポートが開けっ放し，パケットフィルタリングをしていない，パスワードの未設定あるいは弱いパスワード，ログを取っていない，などの脆弱性を持っていることにほかならない。これらは特段難しい処理を要求されるものでなく，基本的な不正アクセス対策を確実に実行し，最新のセキュリティ情報による対策を行えば，多くの被害を未然に防ぐことが出来る。

国を中心とした多くの組織が，インシデント分析技術，生体認証・電子認証，情報漏洩に強い認証・データ管理方式，ネットワーク認証技術の開発を盛んに行っており，その成果が待たれるところである。

4. 2　サイバーテロ（システムに対する犯罪・その 2）

情報通信ネットワークは，いまや国民生活や社会・経済活動における基盤とも言うべき存在となっている。情報通信の分野以外でも，金融，航空・鉄道の運輸，電力・ガス・水道等のインフラ，医療や物流等の各分野，さらには行政サービスの分野でも，情報通信ネットワークの利用が今や不可欠の存在となっている。

4. 2. 1　サイバーテロの脅威

これらの国民生活を支える基幹システムを標的にし，システムの機能不全等をもたらすことを目的とする行為を，サイバーテロと通称する。特に，株式売買や銀行など金融機関のシステム，航空管制や列車運行制御システム，送配電システム等の重要インフラにおける基幹システムが，サイバー攻撃等によってその機能が損なわれた場合には，国民生活や社会・経済活動に大きな混乱をもたらすことは勿論，生命の危機にも直結する重大な影響を与えかねない。

戦争や大規模なテロ活動にも比肩し，社会・経済活動に対する甚大なダメージを招きかねない被害をもたらす可能性を秘めたサイバーテロではあるが，このサイバーテロを行うには，コンピュータとネットワークへのアクセスが確保できれば（勿論，相応の高度な技術知識も必要である),時と場所を選ばず実行が可能であることに問題の深刻さがある。当然のこととして，重要インフラの基幹システムに用いられる通信ネットワークは，そのほとんどがインターネットとは分離され，ないしはクローズドネットワークで運用されている。従って，これらのシステムに侵入することは容易ではないが，日米の政府機関のクローズドネットワークが侵入を許し，ウェブページの改竄などが起きたことを考えれば，深刻な被害を「あり得ないこと」と片付けることはできない。

これまで起きたサイバーテロは，上記に述べたようなインフラに深刻な被害を及ぼす事例は確認されておらず[12)]，ウェブサイトのアクセス超過によるサーバの故障，あるいはウェブページの改竄などがその多くの事例である。

4. 2. 2　対応する法律「電子計算機損壊等業務妨害罪」

サイバー攻撃は，電子計算機損壊等業務妨害罪（刑法234 条の 2）により，処罰対象となる。この条項は，昭和62 年 6 月の刑法改正によって新設されたもので,『人の業務に使用する電子計算機若しくはその用に供する電磁的記録を損壊し，若しくは人の業務に使用する電子計算機に虚偽の情報若しくは不正な指令を与え，又はその他の方法により，電子計算機に使用目的に沿うべき動作をさせず，又は使用目的に反する動作をさせて，人の業務を妨害した者は，五年以下の懲役又は百万円以下の罰金に処する。』と規定された。この罪状が刑法の改正により新設されたのは，これまでの信用毀損および業務妨害罪（刑法 233 条）あるいは威力業務妨害罪（刑法 234 条）では，コンピュータ自体を不正に操作して他人のデータ処理を妨害する行為を，処罰対象として適用することには無理があるとの判断によるものではあるが，法律改正の意図するところは，サイバーテロ等のサイバー犯罪の社会的な重大性を考慮したものであった。

4. 2. 3　サイバーテロに用いられる技法・手段

サイバーテロに用いられる手段としては，ネットへの不正アクセスによることになるが，深刻な被害を招来するのはコンピュータウィルスなどのいわゆる不正プログラムである。

ウィルスには様々な働きをするものがある。多数のコンピュータに感染しその機能を麻痺・停止させ，情報を破壊するもの。また，自己増殖等により膨大な数となったウィルスがインターネットの回線を圧迫し，ネットワーク自体を機能させなくするものもある。さらに，外部記憶媒体に寄生して感染拡大を起こす型もあり，この場合はクローズドシステムネットワークといえども，不正プログラム侵入の可能性を否定できないことになる。

この代表例がボットネットである。ボットネットとは，悪意のある攻撃者によって構築され，インターネット経由の命令によって遠隔操作を可能としたコンピュータ群を指す。ボットネットがサイバー攻撃に使われることになれば，DDos 攻撃（Distributed Denial of Service attack：踏み台と呼ばれる複数のコンピュータが，標的とされたサーバ等に対して Dos 攻撃を行うこと），スパム送信，情報収集（コンピュータに記録されているクレジット番号,メールアドレス,銀行口座等),感染機能をもつため，事態はさらに深刻になることが予想される。ボットに感染した多数のコンピュータから，目的のシステムに対し Dos 攻撃（Denial of Service attack : サーバなどのネットワークを構成する機器に対して攻撃を行い，サービスの提供を不能な状態にすること）が可能となるからである。このボットネットの厄介なところは，トロイの木馬などのウィルスにより，悪意のあるプログラムを使用して多数のコンピュータを乗っ取り，このコンピュータの持ち主が知らないところで，犯罪者の片棒を担ぐ加害者になりうることである。そのため真の犯罪者を特定することが難しいことになる。

またこれまでは，サイバー犯罪は所謂愉快犯が多かったが，このボットネットでは，組織化された犯罪者がボットネットを構築，DDos 攻撃によりビジネス化していることである。現在日本では，30－40 万台のコンピュータが，ボットネットに汚染されているといわれている。

この対策としてウィルス対策ソフトをコンピュータにインストールするのが一般的である。総務省のサイバークリーンセンタでそのためのツールが提供されている。

4. 3　ネットシステムを利用した犯罪

インターネットの急速な普及は，ネットを利用したい

ろいろな形での犯罪（類似行為も含む）行為をも生み出している。銃器や禁止薬物の売買，爆弾の製造方法やテロ用の武器の入手方法の紹介，売春や自殺のサイト，さらには本稿で縷々述べてきたサイバー犯罪の技術手法公開など，様々な形が登場している。

これらの犯罪，犯罪への誘導，犯罪の幇助などがネット上で公然と掲出されることに関しては，規制立法の議論があるものの，「表現の自由」との絡み，また検閲による弊害の問題等からの疑義もあり，未だ議論の域を出ていない。

その一方で，携帯電話を中心としたネット利用が青少年層で急速に拡大しており，「ネット依存症」と呼ばれる社会現象が発生，またそれに関連して各種犯罪行為に繋がると考えられる現象も拡がってきている。青少年保護を吃緊の課題として，ネット上の違法・有害情報対策に対応するいくつかの法律が作られている。ここではそれらのうち，有害情報のフィルタリングを規定した「青少年有害情報規制法」を中心に見ていく。

4. 3. 1 「青少年有害情報規制法」とフィルタリング問題

正式名称「青少年が安全に安心してインターネットを利用できる環境の整備等に関する法律」，通称「青少年有害情報規制法」[13] は平成 20 年 6 月に成立，翌 21 年 4 月に施行された法律である。

法律は，18 歳以下の青少年がインターネットに氾濫する青少年にとって有害な情報と接触する機会を減らすことを目的としている。

具体的には，携帯電話事業者に対し，保護者が申し出た場合を除き，青少年がネットを利用する際にコンテンツフィルタリングサービスを提供することを義務付け（法 17 条），インターネット事業者（＝プロバイダ）には，利用者の求めに応じて青少年有害情報フィルタリングソフトウェア又は青少年有害情報フィルタリングサービスを原則として提供する義務を負わせている（法 18 条）。さらに，サーバ管理者に対しては，青少年にとって有害な情報が発信されていることを知ったときに，青少年の閲覧を防ぐように努めることを規定した（法 21 条）。その他，青少年の安全なネット利用に関する基本方針を定める「インターネット青少年有害情報対策・環境整備推進会議」を内閣府に設置することや，フィルタリングの調査，開発，啓発を行なう団体を第三者機関として認定して，国や地方公共団体が支援することなどが定められている。

● 法律を巡る議論

この法律は，法律案策定の段階から，当事者とされた通信業者及びその団体は勿論，学会やマスコミ，著作権協会，ＰＴＡ，消費者団体などを巻き込んだ広範囲な議論が起きた。

議論は，法律の主旨や目的に対する根本的な疑義，すなわち「法律不要論」と，法律の必要性を認めた上で，その内容に対する問題点を指摘する議論とがある。

法律不要論は，有害情報が青少年の健全な発展に悪影響を及ぼすとする論，また情報の犯罪等への誘因効果に疑問を呈するもので，法律の根拠自体を否定，不要とするものである。同様に教育的観点からの法律不要論もある。すなわち，「適切なインターネットとのつきあい方を教える」ことこそ重要で，「有害」な情報に全くアクセスできない状態で成人した青少年は，どこで情報の取捨選択や主体的な判断といった情報への対応を学ぶのか，あるいはまた，受動的な教育を受けさせるだけでは，興味本位で「有害情報」のサイトを作成する青少年や，成人してから多くの犯罪に巻き込まれる，「情報弱者」が生まれるだけである，などの危惧から立法に反対する議論も見られた。

法律の必要性にまで波及する議論，特に後段の教育的視点，社会的観点からの意見は，法律のあるべき姿の議論としては大いに耳を傾けるべき正論とも言えるが，この議論は本稿の主旨から外れる為，論を閉じ，法律の中身に関する議論を検証することにする。

● 「青少年有害情報」と情報認定の議論

法律の内容についての議論の中心は，フィルタリングの基準となる情報の「有害」性を「誰が判定するのか」ということである。法律のまさに核心部分に関する議論である。情報の「有害」「無害」は個々人によりその判定基準が異なる。その基準が，政府の認める特定の機関に任せられるのでは，「判定基準が恣意的に作られる」可能性があるとする意見が疑義の主たるものであった。

この疑義に配慮し，法律はその理念として，「施策の推進は，自由な表現活動の重要性及び多様な主体が世界に向け多様な表現活動を行うことができるインターネットの特性に配慮し，民間における自主的かつ主体的な取組が大きな役割を担う（一部略）」（法 3 条 3 項）とし，具体的には一昨年 4 月 30 日，携帯電話や PHS のサイトにおける有害情報の排除体制の審査・認定や青少年の保護育成を目的とする，民間有識者等による第三者機関，「モバイルコンテンツ審査・運用監視機構」（略称：EMA）を設立した（法律と同趣旨の条例を持つ地方自治体も多いが，これらの場合にも，それぞれ独自の第三者機関が設立されている）。

法律での「青少年有害情報」は，「インターネットを利

用して公衆の閲覧（視聴を含む）に供されている情報であって青少年の健全な成長を著しく阻害するもの」(法2条3項）と定義する一方，個々の有害情報についての基準は法律では明確に示さず，有害情報の典型的類型を例示するに留めている。そして，法2条4項では，以下のものが「青少年有害情報」として例示されている。

① 犯罪若しくは刑罰法令に触れる行為を直接的かつ明示的に請け負い，仲介し，若しくは誘引し，又は自殺を直接的かつ明示的に誘引する情報

② 人の性行為又は性器等のわいせつな描写その他の著しく性欲を興奮させ又は刺激する情報

③ 殺人，処刑，虐待等の場面の陰惨な描写その他の著しく残虐な内容の情報

※ 条文の解釈は，総務省等による「青少年が安全に安心してインターネットを利用できる環境の整備等に関する法律　関係法令条文解説」を参照されたい。[15)]

● 表現の自由，著作権の侵害

フィルタリングは，基本的人権として憲法21条の保障する「表現の自由」にも抵触するとする意見，また，掲載者（執筆者）の著作権への侵害との意見もある。

表現の自由に関しては，二つの論点があると思われる。一つは，法律の対象とされる者が18歳以下の青少年といえども，憲法21条によって保障される，インターネット上の情報を受領し収集する消極的権利を侵害しないかという問題である。そして，上記の「情報を受領する権利」に制限を加えるとすれば，この法律の内容とする制限が公益上「必要不可欠」かつ「必要最小限」であるか否かがもう一つの論点である。

フィルタリングによって，ネット上のコンテンツを事実上，除去（法律でのフィルタリングはアクセス制限であり，コンテンツの消去ないし除去ではない）することは，コンテンツの著者（掲載者）の著作権を侵害していないかという問題もある。ネット上のコンテンツにも著作権があるのは議論の余地がないが，その内容が事実の報道，また，情報の単なる開示である場合には，著作権の保護対象とはされていない。このことから，本法によってアクセス制限を受ける情報のかなりは，著作権の対象から外れると考えられる。勿論，著作権の対象となる著作物と呼べるコンテンツもある。ここでも二つの議論があった。一つは「違法情報に類するコンテンツ」に著作権があるか，そして「匿名」の場合はどうかである。著作権法における著作権は，著作者に与えられる「財産権」の一種と考えられる。このため，著作権法に「違法」な著作物，あるいは「匿名（作者不詳ではなく作者自身があえて作者名を隠す)」の著作者に関する権利の扱いの条文は見あたらない。(参考＝本稿既述の「プロバイダ責任法」では，名誉毀損などの書き込み情報が発信者不明の場合に，プロバイダ等に削除する権利を認めている。（3．3．2　「プロバイダ責任法」を参照)。大胆な仮説を申し上げれば，「犯罪関与」また「匿名」の創作物であっても著作物としての条件を満たせば，法律の「権原」としては「著作権の対象としての著作物」と考えられるが，著作権が財産権の類型であることから，少なくとも「著作権の主張には無理がある」と考えられよう。

このように考えてくると，規制対象となる有害情報コンテンツで著作権を主張できる要件を満たす著作物は極めて限られ，さらに，本法では対象者の年齢制限を付したアクセス制限の対象とするのであって，ネット上の削除を行うわけではないことから，本法での著作権問題は本法の存立の可否判断，またアクセス規制対象での議論は結びつかない問題と考えられる。

● 法律の実効性に関する議論

議論では，法律の実効性にも対する疑問も挙げられた。その主な論点は，フィルタリングの為に有害とは考えられないサイトまで規制される。有害サイトの多くが海外からの発信（またサイト）であるため国内法で規制はできないのではないか，「ケータイ小説」など，未成年者が関係しているケータイ文化を萎縮させないか，等々が，法律制定に対する疑問点とされて論議された。

フィルタリングは，現時点で統一した基準が出来ないまま，電話事業者やプロバイダに責任を預けた形になっている。理想的には，利用者（または親権者）が適切と考えるフィルタリングのレベルに合わせ，選択的かつ主体的に情報を受信できる様なシステム，また，発信者の情報発信の自由を尊重しつつ，利用者の「知りたい」という権利と，「見たくない」または「(子供に）見せたくない」という利用者の意志を，それぞれ尊重することができる利用者主体の情報システムが構築されることである。

● フィルタリングの方式と技術的課題

フィルタリング技術は，現在極めて積極的に研究・開発されているICT分野の1つである。コンテンツフィルタリングは，接続先のコンテンツ（内容）に問題があれば接続を拒否・遮断する技術である。フィルタリング技術には，接続時にURLだけでコンテンツを判断するURLフィルタリングと，接続のつどコンテンツをチェック，判断する動的コンテンツフィルタリングの2つがある。

これまでは，コンピュータの使用を前提にしたフィルタリング技術が主であったが，最近では，携帯電話の特

に小・中学生への普及を背景に，携帯電話向けフィルタリング技術および，動画像を対象にした技術の開発が活発に行われている。これらは，コンテンツの内容が複雑，大きな情報量をもつ，変化が激しい，などの従来にはない難しさを包含している。2005 年から，携帯電話 3 社は無料で，フィルタリングサービスを開始した。ドコモは，Kid's　i モードプラスサービス，KDDI は，EZ 安心アクセスサービス，ソフトバンクは，ウェブ利用制限サービス，という名称である。特にドコモは，現在もテレビの CM を使い，この安心・安全なフィルタリングサービスの普及を熱心に行っている。

これらの努力に関わらず，現在のところ，発信者の情報発信の自由を尊重しつつ，利用者の「知りたい」という権利と，「見たくない」または「(子供に) 見せたくない」という利用者の意志を，それぞれ尊重する技術は開発されたとは言い難い。

このように，掲示板に書かれた違法・有害情報を検索するフィルタリング技術は，今後さらに重要となる。この進展を加速させた事件が起こった。平成 20 年 6 月の東京秋葉原での通り魔事件である。容疑者は携帯電話サイトの掲示板に約 1000 回，この秋葉原での事件を予告している。さらに，事件当日にも，数十回に渡り，秋葉原で人を殺す，と書き込んでいる。

この他に掲示板では，レンコン 10 万，P 一本 12000，アイス，クリスタル等の隠語を使い拳銃や麻薬の売買が行われている。

このようなインターネットや多様な掲示板での違法・有害情報の検索のため，総務省の外郭団体である独立行政法人情報通信研究機構（通称：NICT）は，平成 21 年から 3 年計画で，インターネット上の違法・有害情報の検出技術に関する研究開発，というテーマで広く研究開発を開始している。ここでは，現在かなりの部分人手に依っている検索機能を，違法・有害情報の辞書を作成することにより，2000 万記事から始まり，400 万記事／月を定常的に追加し，簡単なシステムでの高速な検索を目標にしている。

4. 3. 2　出会い系サイト規制法

インターネットを利用した犯罪に関係する法律をもう一つ簡単に紹介をしておく。

正式名称は「インターネット異性紹介事業を利用して児童を誘引する行為の規制等に関する法律」[14]。平成 15 年に制定されたが，法律制定後も「出会い系サイト」に起因した犯罪が多発していたことから，平成 20 年に出会い系サイト事業者に対する規制強化等の為の改正が行われた。

この法律は，出会い系サイトの利用に起因する児童（18 歳未満）買春その他の犯罪から児童を保護し，児童の健全な育成に資することを目的としており，出会い系サイトを利用する者に対しては，出会い系サイトの掲示板に児童を相手方とする異性交際を求める書き込みをすること（禁止誘引行為）を禁止し（法 6 条），サイト業者に対しては，業の届出，利用者が児童でないことの確認，禁止誘引行為に係る書き込みの削除等の義務を課している（法 3 条，7 条から 14 条までと 16 条）。さらに，プロバイダには，フィルタリングサービスの提供等を（法 3 条 2 項及び 3 項），児童の保護者には，フィルタリングサービスの利用等（法 4 条）の努力規定を設けている。

5．あとがき

現在の ICT 時代では，大容量・高速ネットワークが急拡大し，このネットワークに繋がった PC や携帯電話を国民一人一人が持ち，情報の発信・受信をしている。その代表がインターネットである。確実に我々の生活を便利にしている。ただし，本論文の‘はじめに’でも述べたように，新しい技術には，光と影があることも確かである。これまでの 2 回の論文[1),2)]は，ICT 進展の経済的な問題への影響と法律問題について論述した。今回は，さらに踏み込み，違法・有害情報に代表される ICT の‘命’への影響と，その負の影響を如何に法的に対応できるかについて焦点を当てた。

如何せん，急速な技術の発展と必ずしもフットワークが良くない法律，情報の流通と人権・個人情報の保護という相反する命題での葛藤がこれからも続くと思われる。法的に保護され，我々一人一人が技術の進歩を享受できる社会にして行きたいものである。

謝　辞

本研究の一部は，戦略的研究基盤形成支援事業の援助を受けていることをここに記し，謝意を表します。

参考文献

1）村上仁己，尾形哲志，川崎秀二，「情報通信（ICT）技術の進展と法律問題（その 1)」，成蹊大学理工学研究報告，第 46 巻，第 1 号，51-58 ページ，2009 年 3 月
2）村上仁己，尾形哲志，樋口政和，川崎秀二，「情報通信（ICT）技術の進展と法律問題（その 2)」，成蹊大

学理工学研究報告，第 46 巻，第 2 号，69-80 ページ，2009 年 9 月

3）www.npa.go.jp/cyber/statics/h20/pdf46.pdf：「平成 21 年中のサイバー犯罪の検挙状況等について」平成 22 年 3 月 4 日　広報資料　警察庁

4）http://www.mofa.go.jp/Mofaj/Gaiko/treaty/pdfs/treaty159_4a.pdf

※　ここでは紙数の関係から，個々の犯罪の定義等，条約の内容に触れることはしないが，外務省の全文翻訳が下記アドレスで紹介されているので，参照いただきたい。

※　わが国においても，条約に対処するための国内法整備として「「犯罪の国際化及び組織化並びに情報処理の高度化に対処するための刑法等の一部を改正する法律案」が，平成 16 年，国会に内閣から提出されたが，議論がまとまらず未だに成立を見ていない。

5）http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/m_mail.html

※　「迷惑メール防止法」の条文等は，総務省「電気通信消費者情報コーナー」を参照

※　この法律には数多くの通称，俗称がある。標記した「特定電子メールの送信適正化　法」，あるいは「特定電子メール法」「迷惑メール防止法」などが使われている。

※　シンプルメールトランスファープロトコル（SMPT）＝インターネットやイントラネットで電子メールを送信するためのプロトコル。サーバ間でメールのやり取りをしたり，クライアントがサーバにメールを送信する際に用いられる

※　スパムメール＝広告や嘘の料金請求を目的として送りつけられる電子メール

※　オプトアウトメール，オプトインメール＝オプトアウトメールとは，ユーザの事前承諾なしに送られるダイレクトメールで，例えば，ソフトウェアの登録ユーザ全員にダイレクトメールを送付し，メールの末尾に「以後このメールが必要ない方の連絡先は…」と記載されている場合や，無条件にダイレクトメールが送付される場合だけでなく，ユーザ登録の受付画面において「ダイレクトメールを希望する」があらかじめチェックされている状態になっている場合も，ユーザがダイレクトメールを受け取らないために能動的な行動を起こす必要があることから「オプトアウト」であるとされる場合が多い。

オプトアウトとは逆に，ユーザが自らの意思で広告の受け取りを許諾する方式を「オプトイン」と言い，この方式に従ったメールを「オプトインメール」という。

6）http://www.telesa.or.jp/consortium/provider/：「プロバイダ責任制限法ガイドライン等検討協議会」ガイドライン

7）http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/050526_1.html：「携帯電話不正利用防止法」総務省

8）http://www.npa.go.jp/cyber/statics/h21/pdf53.pdf

※　平成 22 年 3 月 4 日「不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況」（国家公安委員会）

※　「識別符号窃用型」＝アクセス制御されているサーバに，ネットワークを通じて，他人の識別符号を入力して不正に利用する行為（次項，不正アクセス禁止法 3 条 2 項 1 号に該当する行為）をいう。例えば，他人のインターネット・オークション用の識別符号を使用して，当該インターネット・オークションを利用する行為が該当する。

※　「セキュリティ・ホール攻撃型」＝アクセス制御されているサーバに，ネットワークを通じて情報（他人の識別符号を入力する場合を除く）や指令を入力して不正に利用する行為（次項，不正アクセス禁止法 3 条 2 項 2 号又は 3 号に該当する行為）をいう。例えば，セキュリティの脆弱性を突いて操作指令を与えるなどの手法による不正アクセス行為が該当する。

※　フィッシング＝実在する企業を装って電子メールを送り，その企業のウェブサイトに見せかけて作成した偽のウェブサイトを受信者が閲覧するよう誘導し，そこにクレジットカード番号，インターネット上で個人を識別するための ID，パスワード等を入力させて，金融情報や個人情報を不正に入手する行為をいう。

9）http://www.npa.go.jp/cyber/legislation/gaiyou/gaiyou.htm：不正アクセス行為の禁止等に関する法律の概要（警察庁）

10）http://www.microsoft.com/downloads/details.aspx?displaylang＝ja&FamilyID=aa6e0660-dc24-4930-affd-e33572ccb91f

※　2009 年 4 月「マイクロソフトセキュリティインテリジェン　スレポート第 6 版」

11）http://www.npa.go.jp/cyber/statics/h21/pdf53.pdf

12）※　昨年 11 月 7 日，米国のテレビ CBS が，「2007 年にブラジルのエスピリト・サント（Espirito Santo）州で発生し 300 万人以上が影響を受けた大規模停電は，サイバー攻撃が原因であった」と報道し話題を呼んだが，事実関係は明らかではない。

※　本年（2010 年）1 月，Google が，発生源を中国とするサイバー攻撃が行われたと発表。中国当局の検閲問題も絡み，米中両政府を巻き込んだ争いに発展している。（詳細は割愛）

13）http://www.shugiin.go.jp:80/itdb_gian.nsf/html/gian/honbun/houan/g16901030.htm

14）http://www.npa.go.jp/cyber/deai/law/images/law.pdf

※　法律では，「出会い系サイト事業」を「インターネット異性紹介事業」と呼び，以下の 4 要件をすべて満たす事業をいう。①面識のない異性との交際を希望する者の求めに応じて，その者の異性交際に関する情報をインターネット上の電子掲示板に掲載するサービスを提供していること②異性交際希望者の異性交際に関する情報を公衆が閲覧できるサービスであること③インターネット上の電子掲示板に掲載された情報を閲覧した異性交際希望者が，その情報を掲載した異性交際希望者と電子メール等を利用して相互に連絡することができるようにするサービスであること④有償，無償を問わず，これらのサービスを反復継続して提供していること。

15）http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/pdf/095828_1a.pdf