Title	ユビキタス社会におけるサイバー犯罪 : 情報セキュリティの保護法益
Sub Title	
Author	安冨, 潔(Yasutomi, Kiyoshi)
Publisher	慶應義塾大学法学部
Publication year	2008
Jtitle	慶應の法律学 刑事法 : 慶應義塾創立一五〇年記念法学部論文集 (2008.) ,p.281- 306
JaLC DOI	
Abstract	
Notes	
Genre	Book
URL	https://koara.lib.keio.ac.jp/xoonips/modules/xoonips/detail.php?koara_id=BA88453207-00000003-0281

ユビキタス社会におけるサイバー犯罪

——情報セキュリティの保護法益——

安冨潔

一　はじめに

わが国は、明治維新を契機として、農業社会から工業社会へと移行し、第二次世界大戦の終戦を機に、さらに大量生産型の工業社会を急速に発展させ経済大国に成長した。こうした状況にあって、一九六〇年代に始まったコンピュータや通信技術の急速な発展とともに世界規模で進行するＩＴ（情報技術）革命は、一八世紀に英国で始まった産業革命に匹敵する歴史的大転換を社会にもたらした。産業革命では、蒸気機関の発明を発端とする動力技術の進歩が世界を農業社会から工業社会に移行させ、個人、企業、国家の社会経済活動のあり方を一変させたが、インターネットを中心とする情報技術の進歩は、情報流通の費用と時間を劇的に低下させ、高密度の情報の流通を容易にすることにより、人と人との関係、人と組織との関係、人と社会との関係を一変させることとなった。そして、今後、世界は知識の相互連鎖的な進化により高度な付加価値が生み出される知識創発型社会に急速に移行していくと考えられる。そうしたなかでわが国が引き続き経済的に繁栄し、国民全体の更に豊かな生活を実現するためには、情報と知識が付加価値の源泉となる新しい社会にふさわしい法制度や情報通信インフラなどの国家基盤を早急に確立する必要がある。(1)

二〇〇〇年、情報通信技術の利活用により世界的規模で生じている急激かつ大幅な社会経済構造の変化に適確に対応することの緊要性にかんがみ、高度情報通信ネットワーク社会の形成に関する施策を迅速かつ重点的に推進することを目的として、高度情報通信ネットワーク社会形成基本法（平成一二年法律第一四四号）が制定された。

そして、二〇〇一年一月に策定された「ｅ－Ｊａｐａｎ戦略」では、「二〇〇五年までに世界最先端のＩＴ国家となる」という目標のもとで、ＩＴ戦略本部を中心に政府として取り組んできたことで、基盤整備を中心に一応の目標は達成されたと評価できる。(2)しかし、高度情報通信社会においては、いっそうＩＣＴ（情報通信技術）

の発展が課題とされており、さらなる目標達成のために、「e-Ｊａｐａｎ戦略Ⅱ」を通してＩＣＴの利活用に向けて着実に推進されている。もっとも、国民が高度情報通信ネットワーク社会の利便性を十分に享受するためには、安心してインターネット等を利活用できる環境を構築することが必要である。このため、情報通信ネットワークや情報システムについて、その安全性・信頼性及び多様性を確保するとともに、適切な運用管理が図られなければならない。ここに情報セキュリティの確保が求められる理由がある。

他方、今後の社会において解決すべき課題は多く、社会基盤として定着しつつあるＩＣＴの利活用がその課題解決の「切り札」となることを期待し、「いつでも、どこでも、何でも、誰でも」ＩＣＴの利活用ができる社会、いわゆるユビキタス（ubiquitous）[3]・ネットワーク社会の実現に向けた「u-Ｊａｐａｎ政策」が策定され[4]、二〇一〇年を目標に民産学官の有機的連携をもった取り組みがなされている[5]。しかし、ＩＣＴの利活用による利便性の反面、多くの新たな問題も発生するものと予想される[6]。ユビキタス・ネットワーク社会が到来すれば、利用者が享受しうる利便性が飛躍的に増大する一方で、これまで以上に情報主体の権利利益が侵害される事件が発生しうることは想像に難くない[7]。ＩＣＴの恩恵による「光」の部分を享受するためには、「陰」の部分を迅速かつ適正に抑制することが求められる。

本稿では、こうしたユビキタス・ネットワーク社会の到来が期待されるなかで、サイバー犯罪に対する刑事法の役割はいかにあるべきかを考えてみたい。

（1）　ＩＴ戦略会議『ＩＴ基本戦略』一頁（二〇〇〇年一一月二七日）。

（2）　ＩＣＴ（Information and Communication Technology）は、情報（information）や通信（communication）に関する技術（technology）の総称として用いられている。わが国では、これまでＩＴ（Information Technology）という表現が一般的であったが、国

際的にはＩＣＴという用語が普及している。ＩＣＴは、ネットワーク通信による情報・知識の共有が念頭に置かれた表現といえよう。なお、わが国においても、二〇〇四年から総務省が公表している「ＩＴ政策大綱」が「ＩＣＴ政策大綱」と名称を変更するなどしている。

（3）ユビキタスとは、ラテン語の「ubique（あらゆるところで）」という形容詞を基にした、「（神のごとく）遍在する」という意味で使われている英語であるが、ユビキタス・コンピューティングという言葉は、環境中に多くのコンピュータを組み込むことで、いつでも、どこでも、誰でもが、意識しないで、状況に応じた最適な情報の利用ができる情報システムという意味で用いられている。坂村健編『ユビキタスでつくる情報社会基盤』二頁（東京大学出版会・二〇〇六年）。Mark Weiser, The Computer for the 21st Century, p. 94（Scientific American, 1991）.

（4）二〇〇四年七月に総務省が公表したもので、「ユビキタス・ネットワーク整備」、「ＩＣＴ利活用の高度化」、「安心・安全な利用環境の整備」という三つの方向性で議論及び検討がなされている。

（5）u-Ｊａｐａｎ政策パッケージでは、一〇分野（①プライバシーの保護、②情報セキュリティの確保、③電子商取引環境の整備、④違法・有害コンテンツ、迷惑通信への対応、⑤知的財産権への対処、⑥新たな社会規範の定着、⑦情報リテラシーの浸透、⑧地理的デバイドの克服、⑨地球環境や心身の健康への配慮、⑩サイバー対応の制度・刊行の整備）、一〇〇課題について整理し、ＩＣＴに安心感の得られる社会とするように利用環境の整備を図ることとしている。

（6）例えば、証券取引システムや金融機関の現金自動預け払い機や鉄道の自動改札システム等における情報技術の障害、不正アクセスによる重要情報の大量窃取、ファイル共有ソフトやコンピュータ・ウイルスによる重要情報の漏洩などのほか、ボットネット等による情報収集による特定の企業へのスパム攻撃なども報じられている。

（7）フィッシングや迷惑メールにとどまらず、ボット、ゼロディ攻撃、スピアー攻撃、画像スパム、ＵＳＢウイルス、MPack、ルートキッタなどのセキュリティ侵害のインシデントが出現している。

二　情報セキュリティの概念

来るべきユビキタス・ネットワーク社会において、ＩＣＴの利活用による様々な社会経済活動は、基本的にはサイバー空間を介して行われる。したがって、サイバー空間それ自体の安心・安全を確保することが不可欠である。しかし、サイバー空間は、ネットワークなどの電子メディアの中に成立する仮想空間であることから、国家による規制が直接的には及ぶものではなく、ユビキタス・ネットワーク社会におけるさまざまな主体が自律的に関与することによって、安心・安全を確保することが求められている。

このようなユビキタス・ネットワーク社会における安心・安全なサイバー空間を実現するためには、そこで保護されるべき「情報資産」が、正当な利用者にとって、機密性（Confidentiality）、完全性（Integrity）、可用性（Availability）に対する侵害から保護されなければならない。[8]

情報セキュリティは、一般に、情報資産の機密性、完全性及び可用性を維持することと定義されるが、その内容については、必ずしも確立したものとはいえない。ことに、法的な関連性をもって検討されてきてはいるといえるが、わが国では、具体的な規範概念としての内実を伴うものとまでの共通の認識があるとはいえない。[9]

情報セキュリティの概念を「機密性、完全性、可用性」を要素とするものと理解するようになったのは、一九九二年のＯＥＣＤ（経済協力開発機構）の「情報システムセキュリティガイドラインに関する理事会による勧告及び付属文書」においてである。[10] それによれば、「セキュリティの目的」を「情報システムが、その可用性、機密性、完全性に障害（failure）を生じ、そのためにこの情報システムに依存するものに危害（harm）を与える場合に、その危害からそれを保護すること」と定義している。[11] そして、可用性とは、「データ、情報、情報システムが、適時に、必要な様式に従い、アクセスでき、利用できること」、機密性とは「データ及び情報が、権限あ

る者が、権限ある時に、権限ある方式に従った場合のみ開示されること」、完全性とは「データ及び情報が、正確で完全であり、かつ正確性、完全性が維持されること」としている。[12]

また、英国規格協会（British Standards Institute: BCI）が一九九五年に策定したBS7799においても、同様の定義が用いられており、その第一部（Part.1）「情報セキュリティ管理実施基準（Code of Practice for Information Security Management System）」は、情報セキュリティマネジメントを実践する規範として位置づけられ、これは二〇〇〇年に国際標準化機構（ISO）によってISO/IEC17799:2000として国際規格化されている。このISO/IEC17799:2000の定義によれば、[13]情報セキュリティとは、「情報の機密性、完全性及び可用性を維持すること」とされ、機密性とは、「情報にアクセスすることが認可された者だけがアクセスできることを確実にすること」、完全性とは、「情報及び処理方法の正確さ及び完全である状態を保護すること」、可用性とは、「認可された利用者が、必要なときに情報及び関連資産にアクセスできることを確実にすること」と定義されている。[14]さらにISO/IEC17799:2000は、二〇〇五年六月にISO/IEC17799:2005へと改訂されているが、従前の定義はそのまま維持されている。[15]他方、BS7799の第二部（Part.2）「情報セキュリティ管理システム仕様（Specification for Information Security Management System）」は、情報セキュリティマネジメントの認証基準として位置づけられているが、二〇〇二年の改訂を経て、二〇〇五年一〇月にISO/IEC 27001:2005として国際規格化されたが、情報セキュリティについての定義は変更されていない。[16]すなわち、情報セキュリティとは、「情報の機密性、完全性及び可用性を維持すること。さらに、真正性、責任追跡性、否認防止及び信頼性のような特性を維持することを含めうる」とし、機密性とは「認可されていない個人、エンティティ又はプロセスに対して、情報を使用不可又は非公開にする特性」、完全性とは「資産の正確さ及び完全さを保護する特性」、可用性とは「認可されたエンティティが要求したときに、アクセス及び使用が可能である特性」と定義している。

わが国においては、二〇〇五年に情報セキュリティ政策会議が決定した「政府機関の情報セキュリティ対策のための統一基準」において、「機密性、完全性、可用性」概念を用いて政府機関が情報セキュリティ確保のために採るべき対策等を定めている。その中で、機密性とは「情報に関して、アクセスを認可された者だけがこれにアクセスできる状態を確保すること」、完全性とは「情報が破壊、改ざん又は消去されていない状態を確保すること」、可用性とは「情報へのアクセスを認可された者が、必要時に中断することなく、情報及び関連資産にアクセスできる状態を確保すること」と定義している。(17)

このように、情報セキュリティの定義は、一般に、「機密性、完全性、可用性」概念を用いてなされている。(18)

さらに、こうした情報セキュリティの「機密性、完全性、可用性」概念は、二〇〇一年に採択された「サイバー犯罪に関する条約（Convention on Cybercrime）」（以下「サイバー犯罪条約」という。）においても言及されている。すなわち、サイバー犯罪条約の前文において「コンピュータ・システム、コンピュータ・ネットワーク及びコンピュータ・データの秘密性、完全性及び利用可能性に対して向けられた行為並びにコンピュータ・システム、コンピュータ・ネットワーク及びコンピュータ・データの濫用を抑止するために、この条約が必要である」と述べ、「秘密性、完全性及び利用可能性」に対する攻撃を「サイバー犯罪」ととらえることとして、(19)情報セキュリティの保護に関心を寄せている。

（8）坂村・前掲注（3）一四六頁。

（9）アメリカ合衆国では、二〇〇二年に、合衆国法典第四四編第三五章に、「情報セキュリティ」という副章が追加され、情報セキュリティの概念が定義されている（二〇〇二年連邦情報セキュリティ管理法第三五四二条(b)(1)）。また、これにあわせて、国立標準技術研究所法（15U.S.C. 278g-4）二一条も「コンピュータ・システム」を「情報セキュリティ」と改めることとしている。

さらに二〇〇二年国土安全保障法第二編第二二一条以下においても情報セキュリティの強化を図る規定を設けている。

（10）OECD: Guidelines for the Security of Information Systems, C（92）188/Final（1992）。

また、国立標準技術研究所（NIST: National Institute of Standards and Technology）の「情報技術システムセキュリティのための一般的に承認された原則と実務」（Generally Accepted Principles and Practices for Securing Information Technology Systems, 1996）においても、「機密性、完全性、可用性」の概念をセキュリティとして用いている。

（11）もっとも、ここでは、情報セキュリティの一般的定義として用いられている「機密性、完全性、可用性」という順ではなく、「可用性、機密性、完全性」という順で用いられている。

（12）ＯＥＣＤでは、一九八〇年に「プライバシーガイドライン」を公表し、ここでは「機密性、完全性、可用性」という概念は用いられていないが、「安全保護の原則（Security Safeguard Principle）」を掲げており、その具体的内容が分析され、整理された結果、「機密性、完全性、可用性」という概念となったと評価できる。さらに、一九九七年に採択したＯＥＣＤ「暗号政策ガイドラインに関する理事会勧告」においても、暗号は、データの機密性、完全性、及び可用性を保証するものであることを指摘して、「機密性、完全性、可用性」概念に言及している。

（13）ＩＴセキュリティマネジメントのガイドラインであるＧＭＩＴＳ（Guideline for the Management of IT Security; ISO/TR 13355:1997）第一部においては、ＣＩＡに加え、真正性（Authenticity）、説明責任・責任追跡性（Accountability）、信頼性（Reliability）をあげる。真正性（Authenticity）とは、利用者、プロセス、システム及び情報又は資源の身元が主張どおりであることを保証すること、説明責任・責任追跡性とは、主体の行為からその主体にだけ至る形跡をたどれることを保証すること。信頼性とは、意図した動作と結果に整合性があること、と定義する（日本規格協会編『ＪＩＳハンドブック67――情報技術Ⅳ』一一三～一一四〇頁（日本規格協会・二〇〇三年）参照）。

（14）わが国においては、日本工業規格 JIS X 5080:2002 として制定されている。

（15）JIS Q 27002:2006 として制定され、これにより JIS X 5080:2002 は廃止された。

（16）わが国においては、二〇〇六年五月に JIS Q27001:2006 として国内規格化された。

（17）http://www.nisc.go.jp/active/general/pdf/2siryou04-3d.pdf　なお、二〇〇八年に第三版が策定されている。http://www.nisc.go.jp/

active/general/pdf/k303-072.pdf　これらの動向については、http://www.nisc.go.jp/active/general/kijun01.html 参照。

(18)　情報セキュリティの概念については、「機密性、完全性、可用性」という要素で定義することが一般的であるといえるが、技術の進歩にともなう新たな脅威が出現し続けていることから、それらの事象を「機密性、完全性、可用性」概念を用いることによって充分把握できるかには疑問もないわけではないが、議論の整理のための枠組みとしての指標としての意味は残されているし、法制度との関連を論じる上での規範性をもった整理概念としては機能しうるものといえる。岡村久道『情報セキュリティの法律』九頁（商事法務・二〇〇七年）。

(19)　外務省『サイバー犯罪に関する条約』二頁（http://www.mofa.go.jp/mofaj/gaiko/treaty/pdfs/treaty159_4a.pdf）参照。

サイバー犯罪条約は、二〇〇一年一一月八日に欧州評議会閣僚委員会において採択され、わが国は、同月二三日にこれに署名し、二〇〇四年四月二一日に国会で承認した。

サイバー犯罪条約は、サイバー犯罪から社会を保護することを目的として、コンピュータ・システムに対する違法なアクセス等一定の行為の犯罪化、コンピュータ・データの迅速な保全等に係る刑事手続の整備、犯罪人引渡し等に関する国際協力等につき規定するものである（外務省『サイバー犯罪に関する条約の説明書』一頁（二〇〇四年））。

これまでコンピュータ・システム、コンピュータ・ネットワーク及びコンピュータ・データに対する不正行為や犯罪については、コンピュータ犯罪やハイテク犯罪という概念でとらえられてきたが、サイバー犯罪条約では、「コンピュータ・システム、コンピュータ・ネットワーク及びコンピュータ・データの秘密性、完全性及び利用可能性に対して向けられた行為」及び「コンピュータ・システム、コンピュータ・ネットワーク及びコンピュータ・データの濫用」をサイバー犯罪としている。なお、EUでは、二〇〇六年三月一五日の「公開電子通信サービス又は公衆通信網の提供に関連して作成又は処理されるデータ保持に関して指令2002/58/EC を修正する欧州議会・閣僚理事会指令」前文(19)において、サイバー犯罪条約を同指令の趣旨内で保持されたデータを対象とすることとしている。

三　情報セキュリティの刑事法的保護

1　「情報」の法的保護

わが国では、伝統的に、「情報」の法的保護は、情報が記録された媒体を保護することにより、間接的に、なされてきた[20]。しかし、情報は、それ自体、唯一の媒体に記録されている場合を除き、媒体が喪失しても失われることはないという「非移転性」という性格を有するので、その特質に照らした保護がなされるべきであるし、情報は、その内容が多様であり、これに一律の保護を与えることは、実体において異なるものを同じに扱うことになって、実質的に妥当でない結果をもたらすことにもなる[21]。

高度情報通信社会においては、情報は、電磁的に処理され、コンピュータ・ネットワークによってつながれた情報処理システムを流通することから、情報の保護は、「媒体」の保存・管理を通して情報を保護するというあり方から、「情報」それ自体の保存・管理という観点から情報を保護することが必要となってくる。すなわち、ネットワーク化されたコンピュータによる情報処理システムでは情報内容に対して権利を有する者と情報の保存・管理に対して権限を有する者とが乖離するという状況が生じることから、情報の保存・管理へのアクセスの仕方を保護する必要が生じるのである[22]。ここに、情報セキュリティの法的保護が課題となる。

わが国では、一九八七年にコンピュータによる情報処理システムの発展に伴う各種の不正行為に対応するために「刑法等の一部を改正する法律」（昭和六二年法律第五二号）により、いわゆるコンピュータ犯罪に対処するための法整備が図られた。この刑法等の一部改正では、コンピュータによる情報処理に用いられる磁気ディスク等の電磁的記録媒体に保存された記録について、それが従前の文書とは性質を異にするものであることから、「電磁的記録」という文言で、それを「電子的方式、磁気的方式その他人の知覚によっては認識することができない

方式で作られる記録であって、電子計算機による情報処理の用に供されるものをいう」（七条の二）と定義するとともに、電磁的記録不正作出及び供用罪（一六一条の二）、電子計算機損壊等業務妨害罪（二三四条の二）、電子計算機使用詐欺罪（二四六条の二）を新設し、公正証書原本等不正作出罪（一五七条）、公用文書等毀棄罪（二五八条）及び私用文書等毀棄罪（二五九条）の客体に電磁的記録を追加した。その後、カード犯罪の増加に伴い、二〇〇一年の「刑法等の一部を改正する法律」（平成一三年法律第九七号）により、支払用カードを用いた支払システムに対する社会的信頼を保護するために、その準備から使用に至る過程で行われる種々の不正行為に対処するために、支払用カード電磁的記録に関する罪（一六三条の二～一六三条の五）が新設された。

刑法に規定されたこれら一連の構成要件は、基本的に伝統的な処罰規定により対処可能なそれまでの事務処理形態における不正行為と実質的に同様の行為でありながら、コンピュータを用いた新たな事務処理形態による不正行為に対して処罰の間隙を埋めるためのものや、被害の重大性に照らして当時の法定刑では必ずしも十分とはいえない犯罪類型に対して適切な処罰を確保するためになされたものであった。

もっとも、昭和六二年の刑法等の一部改正の際には、保護すべき情報の範囲、保護の程度等について検討を要する問題が少なくないとして、緊急の立法的手当をするうえでは適当でないということで立法が先送りされ[23]、いわゆる情報漏洩という機密性の侵害行為については、刑法に新たな規定が設けられなかった[24]。

その後、コンピュータ・ネットワークを利用した不正行為に対して対処するために、一九九九年に、「不正アクセス行為の禁止等に関する法律」（平成一一年法律第一二八号）（以下「不正アクセス禁止法」という。）による不正アクセス行為の処罰化がなされ、機密性の保護に資する法的規制が実現した。

そして、コンピュータ・ネットワークを利用した情報処理の信頼性確保という観点から、二〇〇二年に、「有線電気通信法」改正（平成一四年法律等一四二号）によるいわゆる「ワン切り」行為の処罰化、及び「特定電子メ

ールの送信の適正化等に関する法律」（平成一四年法律第二六号）による迷惑メール防止のための送信者に対する遵守義務違反の処罰化[25]、二〇〇四年に、「電波法」改正（平成一六年法律第四七号）による暗号通信傍受者による漏示・窃用目的での内容復元行為の処罰化等が図られてきている[26]。

もっとも、わが国での「有体物」に化体した情報の財産的価値を認めるという伝統的な考え方は、客体である有体物である「財物」に情報が化体した場合の価値に言及するもので、情報を有体物から切り離して情報それ自体の財産的価値を保護するものではない。しかし、情報の「非移転性」という特質に照らせば、特定利益の移転を観念しにくいし、仮に対価を観念しうるような情報であったとしても、取得や開示自体が損害発生に直結するわけではないことから、これをいわゆる二項犯罪（刑法二四六条二項、二五九条二項）や背任罪（刑法二四七条）で対処することには限界がある。

2　情報セキュリティの侵害

情報セキュリティの一要素である「機密性」とは、情報にアクセスすることが認可された者だけがアクセスできることを確実にすることであり、機密性の侵害には不正アクセスや情報漏洩の場合がある。

「コンピュータ不正アクセス対策基準」（平成八年通商産業省告示第三六二号）によると、不正アクセスとは「システムを利用する者が、その者に与えられた権限によって許された行為以外の行為をネットワークを介して意図的に行うこと」と定義されている。しかし、法的に規制される不正アクセスは、不正アクセス禁止法八条一号において、三条一項の規定に違反した者を処罰することとしており、技術的な基準と必ずしも整合性をもつものではない。すなわち、不正アクセス禁止法での「不正アクセス」[27]は、電気通信回線に接続された電子計算機であってＩＤ・パスワードによりその電気通信回線を通じた利用ができる者を管理している電子計算機に対し、電気通

信回線を通じて、そのＩＤ・パスワードを窃用し、またはセキュリティホールを利用してアクセスする行為をいうと定義されているからである。[28] もっとも、「不正アクセス」の定義については見解が分かれているが、[29] 不正アクセスは、ネットワークを利用した情報処理の確実性を危殆化するネットワークへの不当な侵入を処罰することと理解する立場は、[30] 情報セキュリティの保護という観点に立脚したものといえる。[31]

機密性の侵害としての情報漏洩については、情報が記録された他人の紙や記録媒体などの有体物を持ち出せば窃盗罪（刑法二三五条）[32] 又は（業務上）横領罪（刑法二五二条、二五三条）[33] が成立することになる。また、事後に事情を知りながらその盗品を譲り受け等すれば盗品譲受け等の罪（刑法二五六条）が成立することになる。もっとも、現行刑法では、電磁的記録それ自体をこれらの罪の客体とせず、これらの罪の客体を有体物としていることから、自己の所持する記録媒体に電磁的記録だけを無断で複写して持ち出しても処罰の対象とならない。この点からも今日の情報社会において、いわゆる「情報窃盗」を処罰する立法が不可欠と考える。

また、「完全性」とは、情報及び処理方法の正確さ及び完全である状態を安全防護することであり、完全性の侵害にはいわゆる情報の改ざんがある。情報の改ざんについては、金融機関におけるオンラインを利用した電子計算機使用詐欺罪（刑法二四六条の二）[34] などがある。

このような故意による完全性の侵害だけでなく、コンピュータの誤操作など過失行為による侵害もみられる。[35] ことに企業や組織における完全性の侵害による損失はその活動に大きな影響をあたえることはいうまでもないのであって、適切な事前のセキュリティ対策が講じられることが重要である。

「可用性」とは、許可された利用者が、必要なときに情報にアクセスできることを確実にすることをいい、可用性の侵害には、いわゆるサービス妨害[36] やシステム侵害[37] があり、電子計算機損壊等業務妨害罪や電磁的記録毀棄罪等がある。[38] もっとも、これらの犯罪は、いずれも故意犯であり、可用性侵害の場合の刑事規制の範囲は限られ

たものといえる。

ところで、サイバー犯罪に関して欧州評議会で採択されたサイバー犯罪条約においては、「装置の濫用」（六条）として、①ハッキングツール等の不正プログラムやコンピュータ・ウイルスについて（六条一項(a)(i)）、②コンピュータ・パスワード、アクセス・コード等について（六条一項(a)(ii)）、それぞれ製造、販売、使用のための調達、輸入、配布、その他の方法によって利用可能とする行為の犯罪化、③右の犯罪を行うために使用する意図をもって①及び②に規定するものを保有する行為の犯罪化を締約国に求めている。しかし、わが国は、不正プログラムの製造等を処罰する規定がないので、①については所要の法整備を行う必要がある。また②についても不正アクセス禁止法ではネットワークで用いるパスワード等に関して罰則規定が設けられているに過ぎず十分とはいえない。さらに③についてもこれに対応する規定はない。したがって、これらを補うための立法が必要である。[39]

コンピュータ・ウイルスは、コンピュータ・プログラムの信用性を害するものとして規制対象とされるもので、その作成・提供をする行為はコンピュータ・プログラムの信用性を害する危険をもたらす危険犯として社会的法益に対する罪といえる。[40] 換言すれば、情報処理の確実性を確保するという意味で、「可用性」侵害の危険犯と位置づけることができよう。

（20）　東京地判昭和五九年六月一五日刑事裁判月報一六巻五＝六号四五九頁（新薬の情報が記載されたファイル）、札幌地判平成五年六月二八日判例タイムズ八三八号二六八頁（住民基本台帳閲覧用マイクロフィルム）、東京地判平成九年一二月五日判例時報一六三四号一五五頁（信用金庫の預金残高明細を印字した用紙）について情報そのものではなく、情報が化体された物を財物と扱っている。

（21）　山口厚「情報の刑法による保護」『情報ネットワークの法律実務2』〔多賀谷一照＝松本恒雄編〕四九〇四～四九〇五頁（第

一法規・一九九九年）。

（22）今井猛嘉「ネットワーク犯罪」法学教室三〇三号四九頁は、ネットワーク犯罪について、①ネットワーク阻害型と②ネットワーク悪用型に分けて、さらに対象の特徴を（α）コンピュータである場合と（β）ネットワークである場合に分けるが、このような立場も、情報保護の特性を考慮するものといえよう。

（23）米澤慶治編『刑法等一部改正法の解説』一四～一五頁（立花書房・一九八八年）。

（24）機密性の保護は、「不正競争防止法」（平成五年法律第四七号）による営業秘密の保護という範囲で保護が図られるにとどまっている。

もっとも、刑法の公正証書原本等不正作出罪、電磁的記録不正作出及び供用罪や電子計算機使用詐欺罪は、主として、完全性を保護するといえるし、電子計算機損壊等業務妨害罪、公用文書等毀棄罪及び私用文書等毀棄罪は、可用性の保護に資するといえる。

（25）特定電子メールの送信の適正化等に関する法律の一部を改正する法律（平成二〇年法律第五四号）により、受信者の同意を得ずに一方的に送信される広告・宣伝目的のいわゆる迷惑メールについてオプトイン方式の導入、実効性の強化等を図り、法人に対する罰金額を一〇〇万円以下から三〇〇〇万円以下に引き上げるなどの改正がなされた。

（26）一九八七年の刑法一部改正の際、不正アクセスは、データの不正操作、データの不正入手・漏示、コンピュータの無権限使用、コンピュータの破壊という行為の予備的手段であり、コンピュータの情報処理機能に対する実質的加害とは必ずしもいえないとして、立法が見送られた（米澤・前掲注（23）一二頁）。

（27）不正アクセス対策法制研究会『逐条不正アクセス行為の禁止等に関する法律』［補訂］六五頁（露木康浩）、一三八頁（檜垣重臣）（立花書房・二〇〇一年）以下参照。

（28）社内ＬＡＮを通じて他人のＩＤ・パスワードを窃用して、サーバにアクセスする行為も不正アクセスとなるが、電気通信回線を通じて行われるものに限られるので、スタンドアローンのコンピュータに不正にアクセスしても不正アクセスには該当しない。また、通常はアクセス制御されているファイルが一時的な設定ミスなどにより自由にアクセスできるようになっている場合、これに電気通信回線を通じてアクセスしても不正アクセスには該当しない。

（29）①電気通信回線を通じて行われる電子計算機にかかる様々な犯罪の予備的行為を処罰する罪と解する見解（不正アクセス対策法制研究会・前掲注（27）二一頁、一三八頁）、②ネットワーク社会における電気通信秩序の維持を危殆化する罪とする見解（園田寿＝牧野二郎＝露木康浩＝前田雅英「ハイテク社会と刑事法（座談会）」現代刑事法八号一七頁（前田雅英）等）、③ネットワーク内でのデータ処理の公共性が認められる場合に限定して不正アクセス罪を認める見解（成瀬幸典「不正アクセス罪についての一考察」阿部純二先生古稀祝賀論文集『刑事法学の現代的課題』三六二頁（二〇〇四年））、④ネットワーク内部でのデータ処理の確実性とそれへの信頼あるいはコンピュータ・データの処理に利害関係を有する不特定多数の者のデータ処理の確実性に対する信頼と解する見解（今井猛嘉「『不正アクセス』の意義をめぐって」研修七一九号九頁、同前掲注（22）五三頁）がある。

（30）今井・前掲注（29）研修一二頁等参照。

東京地判平成一七年三月二五日判例時報一八九九号一五五頁は、不正アクセス行為は、アクセス制御機能の有無については、特定電子計算機ごとに判断するのが相当であり、特定電子計算機の特定利用のうち一部がアクセス制御機能によって制限されている場合であっても、その特定電子計算機にはアクセス制御機能があると解すべきであるとして、ＣＧＩ及びログファイルを閲覧するにはＦＴＰを介して識別符号を入力するものとされていたという事案で、サーバはアクセス制御機能を有する特定電子計算機であるといえるとし、さらに、識別符号を入力してもしなくても同じ特定利用ができ、アクセス管理者が当該特定利用を誰にでも認めている場合には、アクセス制御機能による特定利用の制限はないと解すべきであるが、プログラムの瑕疵や設定上の不備があるため、識別符号を入力する以外の方法によってもこれを入力したときと同じ特定利用ができることをもって、直ちに識別符号の入力により特定利用の制限を解除する機能がアクセス制御機能に該当しなくなるわけではないと解すべきであるとしている。

（31）不正アクセス罪の保護法益について、石井徹哉「不正アクセス禁止法の意義と限界」千葉大学法学論集一九巻三号三一頁は、ネットワークにおける情報処理に関するセキュリティとする。

（32）東京地判昭和六二年九月三〇日判例時報一二五〇号一四四頁等。

（33）東京地判平成一〇年七月七日判例時報一六八三号一六〇頁、東京高判昭和六〇年一二月四日刑事裁判月報一七巻一二号一

一七一頁等。

(34)　大阪地判昭和六三年一〇月七日判例時報一二九五号一五一頁、東京地八王子支判平成二年四月二三日判例時報一三五一号一五八頁、東京高判平成五年六月二九日高刑集四六巻二号一八九頁、名古屋地判平成九年一月一〇日判例時報一六二七号一五八頁等。

(35)　コンピュータへの誤入力の事案として、民事事件で争われたものに、福岡地判昭和五三年四月二一日判例時報九〇一号九〇頁、札幌高判昭和五五年六月二三日判例タイムズ四二一号一〇九頁、東京地判平成一〇年七月一四日金融商事判例一〇六二号五二頁等。

(36)　一般に、サービス妨害は、ＤｏＳ（Denial of Service）あるいはＤＤｏＳ（Distributed Denial of Service）と呼ばれる攻撃によるものである。ＤｏＳ攻撃とはコンピュータに対し、想定していないほど大量のアクセスの繰り返し等を行い、コンピュータのサービス提供を不可能にするなどの攻撃手法をいい、ＤＤｏＳ攻撃は、多数のマシンから同時にＤｏＳ攻撃を行う分散型ＤｏＳ攻撃のことをいう。

浦和地決平成一一年三月九日判例タイムズ一〇二三号二七二頁は、電子メールによるダイレクト・メール送信差止めを求めた仮処分を認めている。

(37)　システム侵害の典型は、コンピュータ・ウイルスである。コンピュータ・ウイルスは、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であり、①自己伝染機能（自らの機能によって他のプログラムに自らをコピーし又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）、②潜伏機能（発病するための特定時刻、一定時間、処理回数等の条件を記憶させて、発病するまで症状を出さない機能）、③発病機能（プログラム、データ等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する等の機能）、という機能を一つ以上有するものをいう（平成七年通商産業省告示第四二九号「コンピュータウイルス対策基準」）。

(38)　大阪地判平成九年一〇月三日判例タイムズ九八〇号二八五頁等。なお、東京地判平成一三年五月二九日判例時報一七九六号一〇八頁は、農林水産省のインターネット掲示板に不正な書き込みを行ったことを内容とする電子計算機損壊等業務妨害被疑事件の捜索・差押えを適法とする。

（39）「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」では、不正指令電磁的記録作成等の罪として、コンピュータ・ウイルス（不正指令電磁的記録作成等）の作成・提供・供用・供用未遂を処罰する規定を定めている。

（40）山口厚『刑法各論』［補訂版］六二八頁（有斐閣・二〇〇五年）、今井・前掲注（22）五七頁。

四　サイバー犯罪と刑事手続

サイバー犯罪では、デジタル化された電磁的記録が重要な証拠となる。

電磁的記録は、「電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、電子計算機による情報処理の用に供されるもの」（刑法七条の二）をいうが、現行の刑事訴訟法は、捜索・差押えの客体を「証拠物又は没収すべき物」（刑訴法九九条一項）としており、一般に、電磁的記録それ自体は捜索・差押えの対象とならないと解されている。(41)

憲法三五条は「住居等の不可侵」を定めるが、その趣旨を、個人の住居や財産に対する物理的な支配権や利用権を保護するものとすれば、電磁的記録は人の知覚によっては認識することができない方式で作られた可視性・可読性のない「情報」であるので、捜索・押収の対象とはならないことになる。しかし、憲法三五条に影響を与えたアメリカ合衆国憲法第四修正の定める「不合理な捜索・押収を受けない権利」について、当初は、個人の住居権や財産権に対する保護として、国家による正当な理由のない物理的な侵入や占有移転を不合理なものとすると解されてきたが、(42)今日では、個人のプライバシーを保護するものであると解されている。(43)すなわち、アメリカ合衆国憲法は、個人のプライバシーの正当な期待を保障しており、個人がプライバシーの期待を現実に表明して

おり（プライバシーの主観的期待）、そのプライバシーの期待が社会にとって合理的で正当なものと認められるものである（プライバシーの客観的期待）場合には、国家は、「相当な理由（probable cause）」及び「捜索場所・押収対象物の明示（particularity）」という実体要件を具備した「令状」が発付されたときに、原則として、捜索・押収することが許されるとするのである。このような立場では、有体物に限らず「情報」も憲法上の保護を受けると解される。

わが国の憲法三五条も、アメリカ合衆国憲法第四修正と同様に、個人のプライバシーを保護していると解するとすれば、可視性・可読性のない電磁的記録それ自体、憲法三五条の保護を受けると解することができよう。[44] もっとも、刑事訴訟法は、捜索・差押えの客体を「証拠物及び没収すべき物」（九九条一項）としているので、電磁的記録は、有体物とはいえないことから捜索・差押えの客体とならないとするのが通説である。そこで、現行法の解釈・運用として、サイバー犯罪の証拠となる電磁的記録を差し押えるには、①証拠となる電磁的記録が記録されている電磁的記録媒体を差し押える、②コンピュータ端末から電磁的記録を出力して（刑訴法一二二条一項・一一一条一項）、プリントアウトしたものを差し押える、あるいはディスプレイに表示させて検証する、③証拠となる電磁的記録を別の電磁的記録媒体に複写して（刑訴法一二二条一項・一一一条一項）、その複写した媒体を差し押える、などの方法がとられてきている。

ところで、サイバー犯罪条約では、自国の権限のある当局が、蔵置されたコンピュータ・データの迅速な保全（一六条）[45]、捜索及び押収並びに提出命令（一八条・一九条）、通信記録のリアルタイム収集並びに通信内容の傍受（二〇条・二一条）を行うことが可能となるよう、必要な立法その他の措置をとる立法義務を課している。[46]

サイバー犯罪条約においては、コンピュータ・システム及びその内部に蔵置されたコンピュータ・データ（一九条一項a）並びにコンピュータ・データ記憶媒体（同項b）に関し自国の領域内において捜索又はこれに類す

るアクセスを行う権限を与えるため、必要な立法その他の措置をとるとして、[47] コンピュータ・データに関して、有体物と区別して、捜索・差押えの権限を自国の権限ある当局に付与することを求めている。[48] また、締約国は、自国の権限のある当局に対し、アクセスしたコンピュータ・データの押収又はこれに類する確保を行う権限を与えるため、必要な立法その他の措置をとる（一九条三項）こととして、「c関連する蔵置されたコンピュータ・データの完全性を維持すること。[49]」及び「dアクセスしたコンピュータ・システムの内部の当該コンピュータ・データにアクセスすることができないようにすること又は当該コンピュータ・データを移転すること。」としているが、これはデータ自体の差押えが可能であることを前提としているとも解されるので、わが国のこれまでの伝統的な有体物を客体とする捜索・差押えに関する法体系においては適切な対応が図られていないといえる。コンピュータ・データという「情報」を対象とする捜索・差押えに関する立法措置が必要であるといえよう。

現行法では、捜索・差押えにあたって、捜索場所や押収対象物を特定することが求められているが、コンピュータ・データ自体を対象とする場合には、物理的な場所や対象を捜索・差押えに先立って特定することは困難である。したがって、コンピュータ・データ自体を対象とした捜索・差押えにおける特定方法や、ネットワークで接続された他のコンピュータへのアクセスの可否などの検討が必要となる。さらに、捜索対象のデータを探し出すこと、そのデータを分離・抽出して複製を作成すること、プリントアウトすること、そして元データにつき、アクセス禁止又は削除などの措置をとることなど、捜索・差押えへの協力の義務づけが必要となると考えられる。[50]

こうした問題点への関心を踏まえ、平成一六年の第一五九回国会に提出された「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」（以下「条約刑法案」という。）においては、捜索差押許可状により特定のコンピュータを捜索したところ、目的とする電磁的記録がそのコンピュータに接続している別のコンピュータに記録・保存されていることが判明した場合に、コンピュータを操作して、必要な電

磁的記録をそのコンピュータあるいは他の記録媒体に複写した上、そのコンピュータ又は記録媒体を差し押えることができるとするいわゆるリモート・アクセスと呼ばれる方法での電磁的記録の収集規定を設けている（条約刑法案における改正刑訴法九九条二項、二一八条二項）[51]。

また、電磁的記録に係る記録媒体の差押え等を行うにあたっては、種々の技術的、専門的な知識が必要な場合が多いことから、捜査機関等が自ら執行することが困難な場合も少なくないし、被処分者の利益の保護等の面からも適当でないことがある。そこで、技術的、専門的な知識を有すると思われる被処分者の協力を得ることができることとしている（同一一一条の二、二二二条一項）。

さらに、ネットワーク・システムでは、電磁的記録が記録されている記録媒体を特定することが困難である場合や、電磁的記録が複数の記録媒体に分散して保管されている場合等において、捜査の目的を十分に達成できないおそれがある。また、プロバイダ等の電磁的記録を保管している者等については、令状があれば、必要な電磁的記録を他のディスク等の記録媒体に記録した上で、その記録媒体を提出する場合も少なくない。このような場合、証拠収集の目的を達するために、電磁的記録を保管する者その他電磁的記録を利用する権限を有する者に命じて必要な電磁的記録を記録媒体に記録させ、又は印刷させた上、当該記録媒体を差し押える「記録命令付き差押え」を新設している（同九九条の二、二一九条一項）[52]。

なお、サイバー犯罪等の捜査においては、その匿名性といった特徴から、犯人の特定等のために通信履歴[53]の電磁的記録を確保することが重要である。サイバー犯罪条約においても、締約国は、自国の権限のある当局に対し、コンピュータ・システムによって伝達される自国の領域内における特定の通信に係る通信記録について（二〇条）、また、自国の国内法に定める重大な犯罪に関しては当該通信の通信内容について（二一条）技術的手段を用いることによりリアルタイムで収集し又は記録する権限を与えるため、必要な立法その他の措置をとることとされて

いる。このようなサイバー犯罪条約の立法義務を受けて、条約刑法案では、保全要請の規定が設けられ、捜査機関が、インターネット・サービス・プロバイダ等に対して、九〇日を超えない期間を定めて、通信履歴の保全を求めることとしている（条約刑法案における改正刑訴法一九七条三項）。

このように、条約刑法案においては、電磁的記録の特質を考慮したあらたな規定が提案されているが、「情報」を対象とする立場での捜索・差押えについての規制原理とはいかなるものであるかについてあらためて検討されなければならないといえよう。

（41）井上弘通「フロッピーディスクに入力された情報の収集と令状の発付」『増補令状基本問題下』〔新関雅夫ほか〕三三一頁（一粒社・一九九七年）、小川新二「磁気のディスクと捜索差押え」『新実例刑事訴訟法』［1］〔平野龍一・松尾浩也編〕二五一頁（青林書院・一九九八年）、田宮裕『刑事訴訟法』〔新版〕一〇二頁（有斐閣・一九九六年）等。

（42）Boyd v. United States, 116 U.S. 616 (1886); Olmstead v. United States, 277 U.S. 438 (1928); Goldman v. United States, 316 U.S. 129 (1942).

（43）Katz v. United States, 389 U.S. 347 (1967).

（44）安冨潔『ハイテク犯罪と刑事手続』一六四頁（慶應義塾大学出版会・二〇〇〇年）参照。

（45）一六条は、締約国は、自国の権限のある当局がコンピュータ・システムによって蔵置された特定のコンピュータ・データ（通信記録を含む。）の迅速な保全を命令すること又はこれに類する方法によって迅速な保全を確保することを可能にするため、必要な立法その他の措置をとることを規定する。

（46）「コンピュータ・データ」とは、コンピュータ・システムにおける処理に適した形式による事実、情報又は概念の表象をいい、コンピュータ・システムに機能を実行させるのに適したプログラムを含む（一条b）なお、サイバー犯罪条約の和訳については、サイバー刑事法研究会報告書『欧州評議会サイバー犯罪条約と我が国の対応について』（経済産業省・二〇〇二年）に

よる（以下、同様）。

（47）一九条一項「締約国は、自国の権限のある当局に対し、自国の領域内において次のものに関し捜索又はこれに類するアクセスを行う権限を与えるため、必要な立法その他の措置をとる。

a　コンピュータ・システムの全部又は一部及びその中に蔵置されたコンピュータ・データ

b　コンピュータ・データを蔵置することができるコンピュータ・データ記憶媒体」

（48）EM（Explanatory Memorandum Related Thereto）184.

（49）なお、コンピュータ・データの完全性の維持という観点から、デジタル・フォレンジック（Digital Forensics）技術の応用が考えられる。デジタル・フォレンジックは、インシデントレスポンスや法的紛争・訴訟に対し、電磁的記録の証拠保全及び調査・分析を行うとともに、電磁的記録の改ざん・毀損等についての分析・情報収集等を行う一連の科学的調査手法・技術のことをいう（デジタル・フォレンジック研究会編『デジタル・フォレンジック事典』四頁（日科技連・二〇〇六年））。捜査においては、「犯罪の立証のための電磁的記録の解析技術及びその手続」をいうと定義される（警察庁『平成一九年警察白書』八六頁（警察庁・二〇〇八年））。

デジタル・フォレンジックは、一九八〇年代からサイバー犯罪や不正行為が生じた場合の証拠収集・保全の技術としてもっぱら捜査機関で用いられてきたが、それだけではなく、今日では、民事事件や企業・組織体にとっても、個人情報や企業情報の漏洩などが起こった場合における自己の活動の正当性を証明する手段として、またセキュリティ確保の証明として用いられている。アメリカ合衆国では、平成一八年の連邦民事訴訟規則の改正によりe-discoveryにおいて活用されている（吉田大介「E―ディスカバリーに関する米国連邦民事訴訟規則の改正」国際商事法務三四巻一一号一四一二頁（二〇〇六年））。

わが国では、デジタル・フォレンジックは「e-Japan重点計画―二〇〇二」における「高度情報通信ネットワークの安全性及び信頼性の確保」のなかで司法手続きのための電子的記録の解析技術に関する系統的な調査研究等を行い、「コンピュータ法科学」分野の確立を目指すとされ、警察庁では犯罪捜査や治安維持の観点から、二〇〇五年に「警察庁情報セキュリティ重点施策プログラム―二〇〇五」を策定し、計算機科学等を利用して、デジタルの世界の証拠性を確保し、法的問題の解決を図る手段としてコンピュータ・フォレンジックに係る取組みの強化をひとつの目標としてきている。

（50）サイバー刑事法研究会報告書・前掲注（46）五二頁。

（51）川出敏裕「コンピュータ犯罪と捜査手続」法曹時報五三巻一〇号一〇頁。

（52）この規定は、通信事業者による記録媒体への記録行為が、第三者に対する免責的効果をもつこととなる。サイバー犯罪条約一八条参照。

（53）通信履歴とは、通信にかかわる事項の記録のうち、通信内容を除いたもの（通信の日時、送信元、送信先などに関する情報）をいう。これに対し、通信内容については、保全対象にならない。

五　おわりに

情報セキュリティが、わが国の法制度において、保護法益としての機能を有するといい得るかはいっそう慎重な検討が必要であろう。(54)

わが国では、伝統的に、生命・身体・財産・名誉等が保護法益とされてきたのであり、ことに財産については、原則として、有体物の保護を中心として考えられてきており、無体情報についての法的保護は、知的財産の場合に例外的に認められているにとどまっている。したがって、情報セキュリティそれ自体を保護法益とすることはいまだ充分とはいえないであろう。しかし、新たな法整備を検討するにあたっては、対象となる情報の保護を介して、終局的にどのような権利利益が保護されるべきかを検討する必要がある。

しかし、来るべきユビキタス・ネットワーク社会においては、ネットワークの脆弱性を踏まえてリスク分析を行い、情報セキュリティを確保するということを基本的な視座として考えていくべきであろう。

ことに、ネットワークの安心・安全を保つためには、情報通信の手段とデータ処理が正確に行われる必要があ

る。ネットワーク機能がいかに優れていても、システムのいずれかの部分に脆弱性があれば、攻撃を受けた場合、全システムが攻撃によって破綻した部分のレベルにまで下がってしまう。そのためには、情報セキュリティの確保は不可欠である。そして、それは、単に技術の問題にとどまらず、法的な制度として構築される必要がある。

慶應義塾創立一五〇年、時代とともに変貌する社会構造にあって、未来先導の社会を構想し、ここに情報化社会における刑事法のあり方についての小論を記念論文集に寄せ、結びとしたい。

(54)　井田良『変革の時代における理論刑法学』一六頁（慶應義塾大学出版会・二〇〇七年）は、高度の技術を悪用した犯罪規制の領域では、早期の刑法的介入の合理性があるが、そこでは法益概念の機能喪失がみられるとして、法益概念を代替・補充する立法上・解釈上の原則を問うべきと指摘する。