産大法学　50巻３・４号（2017.１）

サイバー空間における安全と法

安冨　潔

１　はじめに

情報通信技術の発展は、産業構造や市民生活に大きな変革をもたらした。

第二次世界大戦後、コンピュータと情報通信技術はめざましい進展をとげ、1950年代から1960年代にかけて、商用コンピュータの普及が始まり、1960年代の高度経済成長期のわが国の経済を大きく発展させることとなった。1970年代になると高度経済成長期から安定成長期に移行するが、企業にオフィス・オートメーションの導入が急速に進み、情報システムの信頼性確保が重要となってきた。1980年台になるとパーソナルコンピュータが広く使用されるようになるとともに、本格的にインターネットが普及することとなった。1990年代に入ると、WWWサーバとブラウザの開発・実装がなされ、インターネットの利用が一般利用者にも急速に広がっていった。

今世紀に入ると、P2P（Peer to Peer）技術が実用化され、2005年頃にはSNS（Social Network Service）が開始されるようにり、ネットワークは日常的な情報通信技術として広く社会に定着するようになった。そして、今日、スマートフォンをはじめとするスマートデバイスとクラウド技術の登場によって情報通信ネットワークは社会のインフラストラクチャーとして機能している。

さらに、今後、モノのインターネット（Internet of Thing：IoT）（以下「IoT」と略すことがある。）、ビッグデータ、人工知能（Artificial Intelligence：AI）（以下「AI」と略すことがある。）の進展に伴い、情報通信ネットワーク社会はますます進化するであろう。

このような情報通信技術の飛躍的に進展は、産業の発展と市民生活にお

ける利便性を向上させることとなったが、他方で、情報システムの脆弱性やリスクを悪用したさまざまな出来事が頻繁に発生し、深刻な社会的問題を惹起している。

そこで、情報社会においては、情報システム及び情報通信ネットワークの安全性と信頼性の確保が重要な課題となる。

わが国においては、2000 年に高度情報通信ネットワーク社会の形成に関する施策を推進する目的で「高度情報通信ネットワーク社会形成基本法」（平成 12 年法律第 144 号、以下「IT 基本法」という。）が制定され、「高度情報通信ネットワークの安全性及び信頼性の確保、個人情報の保護その他国民が高度情報通信ネットワークを安心して利用することができるようにするために必要な措置が講じられなければならない。」（第 22 条）こととされた。

その後、情報通信ネットワーク社会の進展とともに、さまざまな情報セキュリティに対する脅威[(1)]が深刻化したことから、いっそうのセキュリティ対策が喫緊の重要な課題となった。

このような情報セキュリティをめぐる社会状況の変化にあって、2014 年サイバーセキュリティに関する施策を総合的かつ効率的に推進するため「サイバーセキュリティ基本法」（平成 26 年法律第 104 号）が制定されたのである。

同法は、情報システム及び情報通信ネットワークの安全性と信頼性の確保という課題に対する法的対応の基本法として位置づけられよう。

本稿は、情報通信ネットワーク社会の進展に伴うサイバーセキュリティに関する法的対応のあり方を素描するものである。

注

（1） システム又は組織に損害を与える可能性のあるインシデントの潜在的な原因（JIS Q13335 : 2006）

2　情報セキュリティとサイバーセキュリティ

(1) 情報セキュリティとサイバーセキュリティの概念

わが国において、情報セキュリティについて定義した法律はない。

しかし、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」と定義されている[(2)]。

情報セキュリティの定義は、1992 年に OECD（経済協力開発機構）が発表した「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勧告」（Recommendation of the Council concerning Guidelines for the Security of Information Systems（adopted by the Council at its 793rd Session of 26-27 November 1992））の付属文書（OECD Guidelines for the Security of Information Systems and Networks Towards a Culture of Security : Annex to the Recommendation of the Council of 26 November 1992）において、「情報セキュリティの目的」は、「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」にあるとしたことから[(3)]、機密性、完全性及び可用性という要素が広く情報セキュリティ概念を表すものして知られるようになった。

OECD のガイドラインでは、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（accurate）で完全（complete）であり、かつ正確さ（accuracy）、完全さ（completeness）が維持されること」と定義している[(4)]。

また、1995 年に英国規格協会（British Standards Institute : BCI）が策定した BS7799[(5)]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、2000 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た。この ISO/IEC 17799 : 2000 では、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[(6)]。

さらに ISO/IEC17799 : 2000[(7)]は、2005 年 6 月に ISO/IEC17799 : 2005 へと改訂されたが、上記の定義は変更されていない[(8)]。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、2002 年に改訂され、2005 年 10 月には ISO/IEC 27001 : 2005 として国際規格化され、これを受けて日本工業規格において、2007 年 5 月 20 日 JIS Q 27002 : 2006[(9)]が制定された。ここでは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、情報セキュリティ政策会議が 2005 年に決定した「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、「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。[10]

他方、こうした技術規格とは別に、法的な観点から、2001 年に採択された「サイバー犯罪に関する条約（Convention on Cybercrime）」においても「機密性、完全性、可用性」概念に言及している。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ー・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ー・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、情報セキュリティの保護という観点から関心を寄せているのである。[11]

このような状況にあって、2000 年に制定された IT 基本法は、高度情報通信ネットワーク社会の形成に関し、基本理念及び施策の策定に係る基本方針を定めた法律であるが、「高度情報通信ネットワーク社会の形成に関する施策の策定に当たっては、高度情報通信ネットワークの安全性及び信頼性の確保、個人情報の保護その他国民が高度情報通信ネットワークを安心して利用することができるようにするために必要な措置が講じられなければならない。」（第 22 条）と高度情報通信ネットワークの安全と安心について言及して、情報通信ネットワークを中心とするセキュリティに関心を寄せているが、情報セキュリティについて既定しているわけではない。

もっとも、情報セキュリティの保護に機能するものといえる個別法がいくつかみられる。例えば、1987 年に「刑法等の一部を改正する法律」（昭和 62 年法律第 52 号）によって「刑法」（明治 40 年法律第 45 号）に新設されたコンピュータ犯罪処罰規定（第 161 条の 2、第 234 条の 2、第 259 条等）や、1993 年の「不正競争防止法」（平成 5 年法律第 47 号）により設けられた営業秘密の保護に関する規定（不正競争防止法第 2 条第 1 項第 4 号～第 9 号、第 10 条、第 13 条、第 21 条第 1 項、第 22 条第 1 項）、1999 年の「不正アクセス行為の禁止等に関する法律」（平成 11 年法律第 128 号、以下「不正アクセス禁止法」という。）、2003 年の「個人情報の保

護に関する法律」（平成 15 年法律第 57 号、以下「個人情報保護法」という。）の個人データ安全管理措置義務に関する規定（第 20 条）などである[12]。さらに、2011 年の「情報処理の高度化等に対処するための刑法等の一部を改正する法律」（平成 23 年法律第 74 号、以下「サイバー刑法」という。）によって、いわゆる「コンピュータ・ウイルス作成罪」（第 168 条の 2）等がサイバー犯罪条約[13]を受けて刑法に新設され、情報セキュリティ保護に寄与するものといえる。

2014 年 11 月 6 日に成立した「サイバーセキュリティ基本法」（平成 26 年法律第 104 号）は、これまでの情報セキュリティという概念を踏まえて、サイバーセキュリティとは「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……（中略）……により記録され、又は発信され、伝送され、若しくは受信される情報の漏えい、滅失又は毀損の防止その他の当該情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置……（中略）……が講じられ、その状態が適切に維持管理されていることをいう」（第 2 条）と定義している[14]。

サイバーセキュリティ基本法は、「インターネットその他の高度情報通信ネットワークの整備及び情報通信技術の活用の進展に伴って世界的規模で生じているサイバーセキュリティに対する脅威の深刻化その他の内外の諸情勢の変化に伴い、情報の自由な流通を確保しつつ、サイバーセキュリティの確保を図ることが喫緊の課題となっている状況に鑑み、我が国のサイバーセキュリティに関する施策に関し、基本理念を定め、国及び地方公共団体の責務等を明らかにし、並びにサイバーセキュリティ戦略の策定その他サイバーセキュリティに関する施策の基本となる事項を定める」（第 1 条）などを目的としている。そして、国の行政機関、独立行政法人[15]及び特殊法人[16]等にサイバーセキュリティの確保について必要な施策を講ずるものとする（第 13 条）ほか、重要社会基盤事業者等におけるサイバーセキュリティの確保の促進（第 14 条）や民間事業者及び教育研究機関等の自発的な取組の促進（第 15 条）などサイバーセキュリティの確保を定め

ている。

(2) サイバーセキュリティ侵害

ア　サイバー攻撃

サイバー空間の安全性を脅かすさまざまな脅威は、サイバー攻撃によって現実社会において顕在化することになる。

サイバー攻撃[17]は、情報システム及び情報通信ネットワークに悪意を持った攻撃者が不正に侵入し、データの窃取・改ざん・破壊、情報システムの作動停止や誤作動、マルウェア[18]の実行や DDoS 攻撃[19]等を行うことで、現実社会に多大なる影響をもたらす。サイバー攻撃は、保護されるべき法益を侵害する結果となることもしばしばである。

サイバー攻撃は、その手法や攻撃対象についてさまざまである。

サイバー攻撃の手法は巧妙化・多様化している[20]。ことに特定の企業や組織をねらって、ウイルス対策ソフトでは検知できない不正プログラムを添付して、業務に関連した正当なものであるかのように装った電子メールを送信し、これを受信したコンピュータを不正プログラムに感染させることで、外部との出口をつくったり、より内部のシステムに侵入を行ったりして、情報の窃取を図る標的型メール攻撃が急増している[21]。

また、サイバー攻撃の対象となり得る範囲も個人や企業等の私的な空間から国や地方自治体等の公的な空間まで広がってきている。今後、重要インフラに対するサイバー攻撃[22]だけでなく、IoT が進展すれば、「モノ」の情報システムへの攻撃も必然となろう[23]。

サイバー攻撃のすべてが「犯罪」となるものではない。しかし、多様なサイバー攻撃に対しては、安全なサイバー空間の確保という観点から、今後、何らかの法的規制が検討されるべきであろう[24]。

イ　サイバー犯罪

サイバー犯罪は、高度情報通信ネットワークを利用した犯罪やコンピュータまたは電磁的記録を対象としてた犯罪等の情報技術を利用した犯罪をいう[25]。

2015 年のサイバー犯罪の検挙件数は、不正アクセス禁止法違反が 373 件、コンピュータ・電磁的記録対象犯罪、不正指令電磁的記録に関する罪が 240 件、ネットワーク利用犯罪（その実行に不可欠な手段として高度情報通信ネットワークを利用する犯罪）が 7,483 件となっている[26]。これは、2014 年に比べて、不正アクセス禁止法違反で 9 件、コンピュータ・電磁的記録対象犯罪、不正指令電磁的記録に関する罪で 38 件、ネットワーク利用犯罪で 134 件の増加であり、過去 5 年でもっとも多かった 2013 年の 8,113 件と比べても 17 件の減に過ぎず、あいかわらず高い数で推移しているといえる。

ことに近年インターネットバンキングに係る不正送金事犯が増加しており、その対策が急務となっている[27]。

また、サイバー犯罪は、インターネットという国境のないサイバー空間におけるネットワークを形成する情報通信技術を悪用する犯罪であることから、国外の被疑者によって実行されたり、海外のサーバを経由・利用して行われることがある。ことに海外サーバは、匿名性が高く、サイバー犯罪の隠れ蓑として利用されることも少なくなく、捜査手法の高度化と国境を越えた捜査における国際共助が求められる[28]。

サイバー攻撃で「犯罪」となるものは、サイバー犯罪として法的規制が及ぶことになる[29]。しかし、サイバー攻撃は、そのほとんどが政府機関、自治体や民間企業等に対して行われる[30]。このようなサイバー攻撃は、国の治安や安全保障だけでなく、重要インフラや企業活動への重大な影響を与えるものであるが、個々の行為について「犯罪」となることがあっても、サイバー攻撃には、①攻撃の実行者の特定が難しい、②攻撃の被害が潜在化する傾向がある、③国境を容易に越えて実行可能であるといった特徴があることから、安全で信頼できるサイバー空間の確保という観点からの総体的な法的規制は容易ではない[31]。

注

（2） 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。しかし、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』〔改訂版〕4頁以下（商事法務、2011）参照。

（3） OECD : Guidelines for the Security of Information Systems, C（92）188/Final（1992）。なお、このOECDのガイドラインでは、「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。また、1997年にOECDが採択した「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。

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）においては、「機密性、完全性、可用性」の概念をセキュリティとして定義している。

（4） OECDが制定した情報セキュリティ関連のガイドラインには、1980年プライバシー保護と個人データの国際流通に関するガイドライン（Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data）、1992年情報システムのセキュリティのためのガイドライン（Guidelines or the Security of Information Systems）（2002年に改正）、1997年暗号政策ガイドライン（Guidelines for Cryptography Policy）がある。

（5） BS 7799は、BS 7799–1（Part1）：「情報セキュリティマネジメントのための実践規範（Code of practice for information security management）」とBS 7799–2（Part 2）：「情報セキュリティマネジメントシステムのための仕様（Specification for information security management systems）」との2部構成となっているが、そのうちpart IのみがISO/IEC 17799としてISO標準とされた。

（6） 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）第一部では、「ITセキュリティマネジメントは、適切なレベルの機密性、完全性、可用性、責任追跡性（accountability）、真正性（authenticity）、及び信頼性（reliability）を達成して維持するためのプロセスである。」と、定義している。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、真正性とは、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、信頼性とは、意図した動作と結果に整合性があることをいう（日本規格協会（編）: JIS ハンドブック 67 ― 情報技術Ⅳ。日本規格協会、113～140 頁（2003）参照）。

（7） Information Technology-Code of practice for information security management.

（8） 2007 年に ISO/IEC 27002 : 2005 と改称されている。

（9） 情報技術 ―― セキュリティ技術 ―― 情報セキュリティマネジメントの実践のための規範（Information technology ― Security techniques ― Code of practice for information security management）は、組織における情報セキュリティマネジメントの導入、実施、維持及び改善のための指針及び一般的原則について規定するとともに、情報セキュリティマネジメントの共通に受容できる目標に関する一般的手引を提供する。

（10） http : //www.nisc.go.jp/active/general/pdf/2siryou04-3d.pdf なお、2008 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。

（11） 外務省『サイバー犯罪に関する条約』2 頁　http : //www.mofa.go.jp/mofaj/gaiko/treaty/pdfs/treaty159_4a.pdf）参照。

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ー・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ー・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ー・データの濫用」をサイバー犯罪としている。

EU では、2006 年 3 月 15 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（DIRECTIVE 2006/24/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC）」前文（20）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。

（12） ガイドラインについて、http : //www.meti.go.jp/policy/netsecurity/secgov-documents.html 参照。

（13） 杉山徳明＝吉田雅之「『情報処理の高度化等に対処するための刑法等の一

部を改正する法律』について」法曹時報 64 巻 4 号 817 頁（2012）。

(14) 国際標準 ITU-T X.1205 においても、ほぼ同様の定義がなされている。Telecommunication Standardization Sector of ITU, “Recommendation ITU-T X.1205 : SERIES X : Data Networks, Open System Communications and Security : Telecommunication security : Overview of cybersecurity,” 2008, p. 2. において、“Cybersecurity is the collection of tools, policies, security concepts, security safeguards, … （中略） … and technologies that can be used to protect the cyber environment and organization and user’s assets. … （中略） … Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user’s assets against relevant security risks in the cyber environment.” と定義されている。

関 啓一郎「サイバーセキュリティ基本法の成立とその影響」知的資産創造 2015 年 4 月号 80 頁参照。

(15) 独立行政法人通則法（平成 11 年法律第 103 号）第 2 条第 1 項に規定する独立行政法人をいう。

(16) 法律により直接に設立された法人又は特別の法律により特別の設立行為をもって設立された法人であって、総務省設置法（平成 11 年法律第 91 号）第 4 条第 15 号の規定の適用を受けるものをいう。

(17) サイバー攻撃の定義は、かならずしも一義的になされてはいない。サイバー攻撃の観測情報を公開している国立研究開発法人情報通信研究機構では、「コンピュータ・ネットワークで構成されるサイバー空間において、不正アクセスやマルウェア感染等により、国家や企業などに損害を与えようとする行為」ととらえている（https : //www.nict.go.jp/press/2012/03/30-1.html#）が、経済産業省商務情報政策局情報セキュリティ政策室「サイバーセキュリティ経営ガイドライン」（2015 年 12 月 28 日）では、「コンピュータ・システムやネットワークに、悪意を持った攻撃者が不正に侵入し、データの窃取・破壊や不正プログラムの実行等を行うこと」としている（http : //www.meti.go.jp/press/2015/12/20151228002/20151228002-2.pdf）

また、警察庁では、重要インフラ（情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス（地方公共団体を含む）、医療、水道、物流、化学、クレジット、石油の各分野における社会基盤）の基幹システム（国民生活又は社会経済活動に不可欠な役務の安定的な供給、公共の安全の確保等に重要な役割を果たすシステム）を機能不全に陥れ、社会の機能を麻痺ひさせるサイバーテロや、情報通信技術を用いた諜ちょう報活動であるサイバーインテリジェンス（サイバーエスピオナージ）に焦点をあててサイバー攻撃ととらえている。警察白書平成 28 年版 120 頁（2016）また、警察庁「焦点」285 号 4 頁（2016. 3）https : //www.npa.go.jp/archive/keibi/syouten/syouten285/pdf/01_2-3P.pdf

(18)　悪意のコード又は悪意のソフトウェアと呼ばれ、利用者の同意を得ずにコンピュータ等にインストールされ（感染）、利用者が意図しない有害な行為を行うプログラムの総称をいう（国立国会図書館調査及び立法考査局『情報通信技術の進展とサイバーセキュリティ』237、102 頁（2015））。なお、JIS Q 27002 : 2014. 12. 2 マルウェアからの保護「情報技術 ―― セキュリティ技術 ―― 情報セキュリティ管理策の実践のための規範」42 頁（http : //kika-kurui.com/q/Q27002-2014-01.html）参照。

(19)　DoS（Denial of Service）は、サービス妨害攻撃のこと。標的となるマシンの処理量や通信量を増加させたり、ソフトウェアの脆弱性や設定の不備を悪用したりして、マシンの機能の低下や停止、あるいはネットワークを利用不可能な状態にすることを意図した攻撃。DoS 攻撃のうち、ネットワーク上の多数のマシンから一斉に行うものを DDoS（Distributed Denial of Service）攻撃という（国立国会図書館調査及び立法考査局・前掲書 216 頁）。なお、DoS,DDoS については、独立行政法人情報処理推進機構『情報セキュリティ教本』〔改訂版〕（土井範久監修）170 頁（実教出版、2009）参照。

(20)　警察庁「平成 27 年におけるサイバー空間をめぐる脅威の情勢について」1 頁（2016 年 3 月 17 日）https : //www.npa.go.jp/kanbou/cybersecurity/H27_jousei.pdf

(21)　2015 年中は、前年下半期から引き続き、「ばらまき型」攻撃が多数発生し、2014 年には 1,474 件（全体の 86%）であったものが、3,506 件（全体の 92%）を占めた。https : //www.npa.go.jp/kanbou/cybersecurity/H27_jousei.pdf

2015 年 6 月、日本年金機構が標的型メール攻撃を受け、同機構が保有する個人情報の一部（約 125 万件）が外部に流出した。

最近の標的型メール攻撃の傾向としては、近年減少傾向にあった「ばらまき型」攻撃が 2014 年下半期に急増しており、商品代金請求等の業務上の連絡を装った英文のものが多くみられた。また、企業等の健康保険組合からの医療費の通知を装うなど、日本の制度を踏まえて受信者が違和感を覚えることのない内容のメールを送信するものもみられた。標的型メール攻撃の送信先アドレスについては、インターネット上で公開されていないものが約 7 割を占めていることから、攻撃者が対象組織や職員について深く調査し、周到な準備を行った上で攻撃を実施していることがうかがわれる。さらに、こうした標的型メール攻撃のほか、対象組織の職員が頻繁に閲覧するウェブサイトを改ざんし、当該サイトを閲覧したコンピュータに不正プログラムを自動的に感染させる手口による「水飲み場型攻撃」や、無償ソフトウェアの更新機能を悪用して不正プログラムに感染させるといった攻撃も発生するなどしている。警察白書平成 28 年版 121 頁。

(22)　国立国会図書館調査及び立法考査局・前掲書 108 頁。

(23)　27 年 6 月以降、複合機のスキャナ機能により読み込んだ文書の送付を

装った標的型メール攻撃がみられる。

(24)　2015 年 6 月に発生した日本年金機構の情報流出事案等を踏まえ、政府機関等のサイバーセキュリティ対策の抜本的強化を図るため、サイバーセキュリティ基本法及び等の改正を行うこととして、国が行う不正な通信の監視、監査、原因究明調査等の対象範囲を拡大するとともに、サイバーセキュリティ戦略本部の一部事務を独立行政法人情報処理推進機構（IPA）等に委託することとして、「サイバーセキュリティ基本法及び情報処理の促進に関する法律の一部を改正する法律」が第 190 回国会に提出され、2016 年 4 月 15 日に可決され、2016 年 4 月 22 日に公布（法律第 31 号）された。http://www.sangiin.go.jp/japanese/joho1/kousei/gian/190/pdf/s031900111900.pdf

湯淺墾道「サイバーセキュリティ基本法の改正」BAN2016 年 10 月号 76 頁。

警察庁のサイバー攻撃に対する対策について、警察白書平成 28 年版 128 頁以下。

(25)　過去 10 年のサイバー犯罪の検挙件数の推移

		2006	2007	2008	2009	2010	2011	2012	2013	2014	2015
不正アクセス禁止法違反		703	1,442	1,740	2,534	1,601	248	543	980	364	373
コンピュータ・電磁的記録対象犯罪・不正指令電磁的記録に関する罪	電子計算機使用詐欺	63	74	220	169	91	79	95	388	108	157
	電磁的記録不正作出・毀棄等	56	34	20	22	36	17	35	56	48	32
	電子計算機損壊等業務妨害	10	5	7	4	6	6	7	7	8	6
	不正指令電磁的記録作成・提供	2011 年刑法改正で追加					0	4	8	9	8
	不正指令電磁的記録供用						1	34	14	16	21
	不正指令電磁的記録取得・保管						2	3	5	3	16
	小計	129	113	247	195	133	105	178	478	192	240
ネットワーク利用犯罪	児童買春・児童ポルノ禁止法違反児童ポルノ）	251	192	254	507	783	883	1,085	1,124	1,248	1,295
	児童買春・児童ポルノ禁止法違反児童買春）	463	551	507	416	410	444	435	492	493	596
	詐欺	1,597	1,512	1,508	1,280	1,566	899	1,357	956	1,133	951
	うちオークション利用詐欺	1,327	1,229	1,140	522	677	389	235	158	381	511
	わいせつ物頒布等	192	203	177	140	218	699	929	781	840	835
	青少年保護育成条例違反	196	230	437	326	481	434	520	690	657	693
	出会い系サイト規制法違反	47	122	367	349	412	464	363	339	279	235
	著作権法違反	138	165	144	188	368	409	472	731	824	593
	商標法違反	218	191	192	126	119	212	184	197	308	304
	脅迫*					67	81	162	189	313	398
	その他	491	752	748	629	775	863	1,106	1,156	1,254	1,593
	小計	3,593	3,918	4,334	3,961	5,199	5,388	6,613	6,655	7,349	7,483
合計		4,425	5,473	6,321	6,690	6,933	5,741	7,334	8,113	7,905	8,096

*脅迫は，2006～2009 年はその他で計上されている　警察庁統計より
http : //www.npa.go.jp/cyber/statics/h22/pdf01.pdf
http : //www.npa.go.jp/kanbou/cybersecurity/H27_jousei.pdf

(26)　警察庁「平成 27 年におけるサイバー空間をめぐる脅威の情勢について」9 頁。

(27)　被害額は、2014 年に約 29 億 1,000 万円と過去最高となったが、27 年には約 30 億 7,300 万円と 26 年を上回っている。被害の特徴としては、被害金融機関数が倍増し、特に信用金庫、信用組合に被害が拡大したこと、農業協同組合と労働金庫で被害が発生したこと等が挙げられる。警察庁「平成 27 年におけるサイバー空間をめぐる脅威の情勢について」6〜7 頁。

(28)　2015 年 11 月、茨城県警察など 18 都道府県警察において、海外サーバを利用したアダルトアフィリエイトサイトに係る一斉集中取締りを実施し、わいせつ電磁的記録記録媒体陳列により 13 人を検挙した事例や、京都府警察において、発売前の週刊漫画雑誌の誌面をデジタル化した上で海外サイトに蔵置してインターネット利用者に無料公開していた被疑者 6 人を著作権法違反で検挙した事例がある。警察庁「平成 27 年におけるサイバー空間をめぐる脅威の情勢について」8 頁。

(29)　2015 年 7 月に、携帯電話アクセサリー販売会社に DDoS 攻撃行い、業務を妨害したとして、電子計算機損壊等業務妨害容疑でベトナム人が逮捕されている（警視庁）。また、2015 年 11 月には、政府機関に対する不正アクセス事件に関して、犯行に使用されたレンタルサーバの契約に際し、当時日本に留学生として在留していた中国籍の男性が、氏名、住所、生年月日等、虚偽の情報により会員登録を行っていた事実が判明したことから、私電磁的記録不正作出・同供用罪により検挙されている。さらに、2016 年 6 月 27 日には、佐賀県内の県立中学や高校の生徒らの成績をインターネット上で管理するシステムなどに侵入し、成績など個人情報を含む約 21 万件のファイルを盗み取ったとして、不正アクセス禁止法違反の疑いで、佐賀市の 17 歳の無職少年を逮捕している（警視庁・佐賀県警）。

(30)　主要なものだけでも、2015 年 5 月 8 日から 5 月 18 日に日本年金機構が標的型メール攻撃を受け、年金情報管理システムに対して、外部の不正アクセスがなされ、約 125 万件の個人情報が流出した事件（http : //www.nenkin.go.jp/oshirase/topics/2015/0104.files/F.pdf）や、同年 11 月 21 日から 23 日にかけて厚生労働省のウェブサイトが外部から DDoS 攻撃を受けウェブサイトが一時停止した事件（http : //www.security-next.com/064491）などのほか、2016 年には、1 月 12 日から 13 日にかけて日産自動車のウェブサイトが DDoS 攻撃を受け、一時的に停止した事件（http : //www.security-next.com/065976）、同年 2 月 27 日に京都動物愛護センターのウェブサイトが不正アクセスを受けて改ざんされ、閲覧するとマルウェアへ感染するおそれがあった事件（http : //www.security-next.com/067349）、同年 4 月 20 日に日本テレビのウェブサイトで利用する脆弱性があったソフトウェアが不正アクセスを受け、最大 43 万件の個人情報が漏洩した事件（http : //www.ntv.co.jp/info/pressrelease/index20160421.html）、同年 6 月 2 日に群馬県が利

用する端末1台がマルウェアに感染し、外部と不正な通信を行っていた事件（http : //www.pref.gunma.jp/houdou/b2800017.html）、同年6月29日から30日にかけて千葉県柏市で複数の事務用端末が標的型メール攻撃を受けマルウェアに感染し、外部と不正な通信を行っていた事件（http : //www.city.kashiwa.lg.jp/soshiki/020300/p035929.html）など、さまざまな分野におけるサイバー攻撃が報告されている。http : //www.security-next.com/category/cat191/cat27 など参照。

(31) Brewster, Ben Akhgar, Babak, *Combatting Cybercrime and Cyberterrorism : Challenges, Trends and Priorities,* Springer International Publishing, 2016

3　情報通信技術の進展とセキュリティ

情報システム及び情報通信ネットワークの進展に伴い、サイバー空間という仮想社会とフィジカル空間という現実社会とが融合することによる新たな経済産業社会システムが政府による「日本再興戦略2016」として提言されている(32)。

このようなサイバー空間と現実空間が融合した社会では、IoT、ビッグデータ、AIなど新たな情報通信技術が経済成長に貢献するものとして期待されているが、その企図するところが実現できるためには情報システム及び情報通信ネットワークのセキュリティが重要となる。

(1)　モノのインターネット（IoT）

モノのインターネット、IoTとは“Internet of Things”の略である。

国際電気通信連合（International Telecommunication Union : ITU）の勧告では、IoTについて「情報社会のために、既存もしくは開発中の相互運用可能な情報通信技術により、物理的もしくは仮想的なモノを接続し、高度なサービスを実現するグローバルインフラ」とされ、次のようなことが期待されている(33)。

①「モノ（Things）」がネットワークにつながることにより迅速かつ正確な情報収集が可能となるとともに、リアルタイムに機器やシステ

ムを制御することが可能となる。

②カーナビや家電、ヘルスケアなど異なる分野の機器やシステムが相互に連携し、新しいサービスの提供が可能となる。

IoT は「モノ」がネットワークにつながって新しい価値を生むだけでなく、IoT が他の IoT とつながることでさらに新しい価値を生むという複雑化する統合システム（System of Systems : SoS）としての性質を持っている。[34]

IoT には、①脅威の影響範囲・影響度合いが大きいこと、② IoT 機器のライフサイクルが長いこと、③ IoT 機器に対する監視が行き届きにくいこと、④ IoT 機器側とネットワーク側の環境や特性の相互理解が不十分であること、⑤ IoT 機器の機能・性能が限られていること、⑥開発者が想定していなかった接続が行われる可能性があることという特質があることが指摘されている。[35] こうした特質は、サイバーセキュリティの脆弱性とも関連して、さまざまな脅威を内包するものであり、IoT の実装にあたってのセキュリティの確保が必要となってくる。[36]

ところで、IoT のシステムを実現するには組込みシステムが必要となる。

組込みシステムとは、機器に組み込まれた半導体やその周辺装置からなる部分で、機器の制御を行う目的に専用化されたコンピュータ・システムである。[37] 組込みシステムは、情報通信技術の進展により、インターネットなどのオープンなネットワークに接続されるようになりつつあることによって、パソコンと同様に、ネットワークを介した第三者による攻撃の脅威にさらされる可能性が高まっている。[38]

このように IoT 機器やシステムがネットワークに接続して動作できるようになると、サイバー攻撃やシステム障害が発生するなどによって安全に影響を及ぼしたり、個人の生活データなどの重要な情報が漏えいしたりする可能性がある。[39]

インターネットに接続された「モノ」はすべて攻撃対象となる。たとえ直接の攻撃目標とならなくても、踏み台として利用されることもある。[40]

(2) ビッグデータ

ビッグデータとは多種多量なデータを意味するが、情報通信システムの進展により、大量のデータが収集、蓄積され、それをリアルタイムに分析することによりビジネスに利活用する事例が増えているが、他方で個人情報を含むパーソナルデータの扱いに関するセキュリティやプライバシーの問題が発生している。

例えば、東日本旅客鉄道株式会社の提供するSuicaに関するデータに基づき、株式会社日立製作所が駅のマーケティング資料を作成・販売する事業につき、東日本旅客鉄道の保有するSuica乗降履歴データを変換したものを日立製作所に提供しようして、個人情報の取り扱いについて批判を浴び、取り止めたケースがある[41]。この事案では、東日本旅客鉄道が日立製作所に提供しているSuicaに関するデータは、Suicaでの乗降駅、利用日時、鉄道利用額、生年月、性別及びSuicaID番号（Suicaに割り振られた固有の番号）を他の形式に変換した識別番号からなるSuica利用に関するデータである。これらのデータには氏名や連絡先は含まれておらず、個人を特定することはできないとはいえ、プライバシーの保護という観点から疑問が呈されたのである。

ビッグデータには個人に関する情報やそれに相当するデータが含まれている場合も多い。個人に関する大量の情報が集積、利用されることによる個人情報及びプライバシーの保護に関する懸念もあり、「個人情報保護法」では規律できない場合もある。

匿名化技術を適用しても個人が特定されるリスクは残ることから、そうしたリスクを踏まえて個人情報の利活用を行うためには、制度の整備が必要となってくる[42]。

ビッグデータに関しては、インターネット上で自らのプライバシーをどのように守るか。個人の情報が蓄積され、紐付けられることによって、想定もしていない人に想定もしていない目的で利用されているかも知れないということに留意する必要がある。

(3) 人工知能

「人工知能」(Artificial Intelligence : AI) は、一般的に言えば、推論・判断などの知的な機能を人工的に実現するための機能を備えたコンピュータ・システムのことをいう[43]。

AI はさまざまな分野で今後いっそう研究が進み、情報システム及び情報ネットワークにおいて実装されるであろう[44]。

ことにサイバー攻撃からの脅威に対して既存技術による対策では完全な防御は困難であることから、人工知能に用いてさまざまなシステムのログやイベントを統合管理し、横断的に相関分析することで、脅威をいち早く検知・対処する研究がなされ[45]、セキュリティ事業者によってサービスが提供されている。

情報社会が発展するなかで、AI がネットワークと連結され、「AI ネットワーク化により AI の自律的判断に基づく動作に起因する法的問題が増大することなどにより、権利義務及び責任の帰属主体、法律行為及び不法行為並びに犯罪に関する法制度など従来の社会の基本ルールの在り方の見直しが求められる可能性がある。」[46]

注

(32) http : //www.kantei.go.jp/jp/singi/keizaisaisei/pdf/2016_zentaihombun.pdf

(33) ITU-T Y.2060 (ITU-T Y.4050 on 2016-02-05)。https : //www.itu.int/rec/T-REC-Y.2060-201206-I

(34) http : //www.meti.go.jp/press/2016/07/20160705002/20160705002-1.pdf

(35) http : //www.soumu.go.jp/main_content/000421617.pdf

(36) 総務省・経済産業省 IoT 推進コンソーシアム「IoT セキュリティガイドライン ver 1.0 (案)」(平成 28 年 5 月) http : //www.soumu.go.jp/main_content/000421617.pdf

(37) 組込みシステムは、産業機器や家電製品、自動車などの機器に組み込まれ、様々な分野で利用されている。

国立国会図書館調査及び立法考査局『情報通信技術の進展とサイバーセキュリティ』138 頁 (2015)。

(38) 海外で「Symbian OS」を搭載した携帯電話に感染するウイルスの発見や ATM 等の専用システムが感染しサービス不能に陥った事案が報告されてい

る。鵜飼裕司「組込みシステムのセキュリティの現状と対策 ―― 具体的な脅威と対策の提案 ――」https : //www.ipa.go.jp/files/000009699.pdf

わが国においても、2014 年 6 月に POS システムのマルウェア感染が確認されたと報道されている（毎日新聞「POS：ウイルスまん延　レジと一体、カード情報危険に　国内で検出数急増、感染も」2014. 6. 30、夕刊」。

情報処理推進機構「組込みシステムのセキュリティへの取組みガイド（2010 年度改訂版）」2010. 9、http : //www.ipa.go.jp/files/000014117.pdf

(39) IoT についてプライバシーやセキュリティに関心を寄せたものとして、Delgado, Emanuel, *Internet of Things : Emergence, Perspectives, Privacy and Security Issues*, New York : Nova Science Publishers, Inc., 2015 や Hu, Fei, *Security and Privacy in Internet of Things (IoTs) : Models, Algorithms, and Implementations*、Boca Raton : CRC Press, 2016 などがある。

また、法的視点から論じたものとして、Weber, Romana & Weber, Rolf H., *Internet of Things : Legal Perspectives,* Springer Berlin Heidelberg, 2010 がある。

(40) 読売新聞は「インターネットにつながる世界中の監視カメラや火災報知機などの IoT 機器約 15 万台がウイルスに感染し、サイバー攻撃の「踏み台」となっている」との記事を配信している（2016. 3. 21 東京朝刊社会面）。

また、警察庁では、2015 年 12 月 15 日「IoT 機器を標的とした攻撃の観測について」として、IoT（Internet of Things）機器を乗っ取ってボット化させるサイバー攻撃の観測結果を公表している。これによれば、攻撃にさらされているのはルーターや Web カメラ、ネットワークストレージ、DVD レコーダー/BD レコーダーといった、組み込み Linux を搭載してインターネットに接続する機器で、Telnet で利用される TCP の 23 番ポートに対する高頻度のアクセスがみられ、攻撃の踏台として悪用されているとしている。https : //www.npa.go.jp/cyberpolice/detect/pdf/20151215_1.pdf

(41) http : //www.jreast.co.jp/press/2013/20130716.pdf

(42) 高度情報通信ネットワーク社会推進戦略本部「パーソナルデータに関する検討会」（技術検討ワーキンググループ）「技術検討ワーキンググループ報告書」4 頁（2013/12/10） http : //www. kantei.go.jp/jp/singi/it2/pd/dai5/siryou2-1.pdf

(43) 人工知能の概念は、1947 年に「ロンドン数学学会における講演」（Lecture to London Mathematical Society）においてアラン・チューリングが提唱したとされており、その後 1956 年の「人工知能に関するダートマスの夏期研究会」（The Dartmouth Summer Research Project on Artificial Intelligence）において、初めて「人工知能」という言葉が用いられたとされる。

人工知能については、松尾豊ほか『人工知能とは』人工知能学会監修（近代科学社、2016）、松尾豊『人工知能は人間を超えるか　ディープラーニングの先にあるもの』（（角川 EPUB 選書）、2015）など。

（44）　例えば、アップルやグーグルが提供するパーソナルエージェントサービスは、スマートフォン等に組み込まれ、世界中に急速に普及しつつある。http : //www.soumu.go.jp/main_content/000424360.pdf

（45）　マサチューセッツ工科大学（MIT）のコンピュータ科学および人工知能研究所（Computer Science and Artificial Intelligence Laboratory ; CSAIL）が「AI Squared」（AI2）と呼ばれるそのプラットフォームを開発し、85%の攻撃を検知（現在のベンチマークの約 3 倍の確率）するほか、偽陽性も 5 分の 1 に減らすとしている。https : //www.csail.mit.edu/System_predicts_85_percent_of_cyber_attacks_using_input_from_human_experts%20

人工知能は、その性能が全人類の知性の総和を越える「（技術的）特異点、シンギュラリティ」（Technological Singularity）と呼ばれるものが、2045 年に来ると予測されている。Ray Kurzweil, The Singularity Is Near : When Humans Transcend Biology, New York : Penguin Books, 2006

（46）　総務省 AI ネットワーク検討会議「AI ネットワーク化の影響とリスク――智連社会（WINS ウインズ）の実現に向けた課題――」報告書 2016（2016/6/20）57 頁 http : //www.soumu.go.jp/main_content/000425289.pdf

4　おわりに

情報システム及び情報通信ネットワークの普及により地球的規模で「インターネット」というのひとつの空間が構築されている。この空間では、サイバー社会というこれまでにない社会を形成する。サイバー社会では国家主権に基づく法域はない。しかし、サイバー社会は、人々にとって不可侵の「聖域（sanctuary）」であってはならない。サイバー空間が現実空間と連接することで、サイバー社会もまた現実社会とつながっているのである。

サイバー社会においても、個人の権利・利益を侵害してはならないし、市民生活に不可欠なインフラを毀損してはならない。

そこで、現実社会と連接した情報器機やソフトウェアに対する法的規制によりサイバー社会の安全・安心を実現していくこととなろう。

これから情報システム及び情報ネットワークがいっそう進展し、さまざまなモノがネットワークでつながり、大量の情報が収集・蓄積・利用され、人工知能による情報処理が普及していくことが想定される。

情報システム及び情報ネットワークに無謬はない。可能な限りの安全対策を施した情報システム及び情報ネットワークが実装されなければならない。しかし、技術的な安全対策だけでは、サイバー社会の安全・安心を実現することはできない。

サイバーセキュリティの確保は安全・安心なサイバー社会を築くうえで不可欠の課題であり、そのためにどのような法的規制がなされるべきかを考えていなければならないのである。