Ⅱ-6
サイバーセキュリティの社会的側面

6.1　プライバシー

6.1.1　パーソナルデータ

個人に関連する様々なデータ（パーソナルデータ）をビッグデータとして解析することで生まれるイノベーションを活発化すべく、個人情報保護、プライバシー保護に関する課題を整理し、制度改正に向けた基本的な枠組みを提案する「パーソナルデータの利活用に関する制度改正大綱」が2014年6月に決定された。

「個人情報」と「プライバシー」は区別せず使用される場合があるが、厳密には異なる概念である。「個人情報の保護に関する法律」（いわゆる「個人情報保護法」。平成15年法律第57号）第2条第1項では、「個人情報」を「生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）」と定義している。つまり、個人が特定可能である本人に関わる全ての情報である。

一方、「プライバシー」という言葉自体は法令上で定義されていないが、「宴のあと」事件の東京地方裁判所昭和39年9月28日判決では、日本国憲法第13条に基づく「私生活をみだりに公開されないという法的保障ないし権利」との定義が示され、他の判例もこの定義を踏襲している。

近年、ライフログ（携帯端末等で取得・蓄積された活動記録情報）等、個人に関する情報を含むビッグデータを利用するビジネスが活発化し、パーソナルデータ(1)の利用価値が高まっている一方で、個人情報保護とプライバシー保護に対する社会の目はこれまで以上に厳しくなっている。パーソナルデータは、そのデータ単体では個人を識別することができないものであっても、ほかの情報と照合された場合、個人の識別に結び付く可能性がある。また、多くのデータを収集したり、分析したりすることで個人の生活習慣、行動範囲、嗜好を特定できる可能性があり、パーソナルデータの利活用におけるプライバシー侵害に対する懸念が高まっている。

このような懸念を解消し、経済活性化に向けたパーソナルデータ利活用に対応するため、高度情報通信ネットワーク社会推進戦略本部（IT総合戦略本部）は、2013年6月の決定に基づき、同年9月に、パーソナルデータに関する利活用ルールの明確化を目的とした「パーソナルデータに関する検討会」を設置した(2)。同検討会の活動成果として、「パーソナルデータの利活用に関する制度改正大綱」が、2014年6月24日、IT総合戦略本部によって決定された(3)。同大綱では、パーソナルデータの利活用に向けた基本的な枠組みとして、①本人の同意なしにデータの利活用を可能とする「個人の特定性を低減したデータ」(4)への加工と本人の同意の代わりとしての取扱いの規定、②「個人情報」の範囲の明確化とその取扱いの規定等の基本的な制度の整備及びこれを補完する民間の自主的な取組の活用、③法定事項や民間における自主的な取組について実効性ある執行を行うための、国際的な整合性も確保した第三者機関の設置等が示されている。

本大綱に基づき、法案作成の参考とするためのパブリックコメントが、2014年6月25日から7月24日にかけて実施され、213名から1,051件の意見が寄せられた。前述のパーソナルデータの利活用に向けた枠組みについて、賛否両論の意見が集まっており、企業及び個人における個人情報保護に関する関心の高さがうかがえる。政府は、このパブリックコメントの意見を踏まえ、2015年の第189回国会に個人情報保護法の改正案を提出する予定としている。

●事例研究

■Suica履歴情報の外部提供

2013年6月、東日本旅客鉄道（JR東日本）が提供する電子マネーSuicaの履歴情報を匿名化処理を施した上で日立製作所に提供する事業について両社が発表を行った(5)。日立製作所は、首都圏の駅におけるSuicaの履歴情報に基づき、各駅エリアの利用者の利用目的、利用状況等を分析し、店舗の出店計画や立地評価、広告・宣伝等の事業に活用することを計画していた(6)。しかし、事業の発表後、Suicaの利用者やメディアから、プライバシーの保護や消費者意識に対する配慮が欠けているとの批判や不安視する声があがり、事業継続を見合わせることとなった。

JR東日本が設置した社外の専門家からなる有識者会議は、同事業により直ちに個人のプライバシーが侵害されるおそれはないと判断したが(7)、このような事例が注目を集めることで、事業者が社会的批判を懸念して、パーソナルデータを利活用した事業を躊躇してしまう状況もあり、保護すべき情報の範囲や事業者が遵守すべきルールを明確にすることが急務となっている。

●海外の状況、技術動向、制度、規制

■データ保護プライバシー・コミッショナー国際会議

2014年10月、各国のデータ保護当局が集まり、プライバシー保護に関する議題について意見交換を行うデータ保護プライバシー・コミッショナー国際会議の第36回会合がモーリシャスで開催され、モノのインターネット（IoT）に関する宣言（Mauritius Declaration on the Internet of Things）(8)とビッグデータに関する決議（Resolution Big Data）(9)が採択された。IoTに関する宣言では、IoTから生成されたデータはパーソナルデータに該当し、IoT機器を提供する事業者に、収集されるデータの取扱の明確化や適切なセキュリティ対策の実施を求めている。また、ビッグデータに関する決議では、ビッグデータを利活用する事業者に対して、データの当事者に、収集されたデータ及びデータの分析アルゴリズムへのアクセス権を与えることを求めている。

---

(1)　個人識別性を有する「個人情報」に限定されず、広く「個人に関する情報」と定義されている。総務省パーソナルデータの利用・流通に関する研究会「パーソナルデータの利用・流通に関する研究会報告書―パーソナルデータの適正な利用・流通の促進に向けた方策―」2013.6, p.6. 総務省ウェブサイト <http://www.soumu.go.jp/main_content/000231357.pdf>

(2)　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の開催について」2013.6.14. <http://www.kantei.go.jp/jp/singi/it2/kettei/pdf/20130614/siryou2.pdf>

(3)　高度情報通信ネットワーク社会推進戦略本部「パーソナルデータの利活用に関する制度改正大綱」2014.6.24. <http://www.kantei.go.jp/jp/singi/it2/info/h260625_siryou2.pdf>

(4)　大綱では、個人が特定される可能性を低減したデータの取扱に関して具体的な内容は示していないが、2013年の総務省の研究会では、米国連邦取引委員会の考え方に基づき、本人の同意を得なくてもパーソナルデータの利活用を行うことができる条件として、①適切な匿名化措置を施していること、②匿名化したデータを再識別化しないことを約束・公表すること、③匿名化したデータを第三者に提供する場合は、提供先が再識別化をすることを契約で禁止することの全てを満たす場合と提示している。 総務省パーソナルデータの利用・流通に関する研究会　前掲注(1), p.33.

(5)　Suicaに関するデータの社外への提供についての有識者会議「Suica に関するデータの社外への提供について中間とりまとめ」2014.2, pp.3, 7-10. 東日本旅客鉄道ウェブサイト <http://www.jreast.co.jp/chukantorimatome/20140320.pdf>

(6)　「交通系ICカードのビッグデータ利活用による駅エリアマーケティング情報提供サービスを開始」2013.6.27. 日立製作所ウェブサイト <http://www.hitachi.co.jp/New/cnews/month/2013/06/0627a.html>

(7)　Suicaに関するデータの社外への提供についての有識者会議　前掲注(5), pp.12, 20.

(8)　“Mauritius Declaration on the Internet of Things,”October 14, 2014. 36th International Conference of Data Protection and Privacy Commissioners Website <http://www.privacyconference2014.org/media/16421/Mauritius-Declaration.pdf>

(9)　“Resolution Big Data.”36th International Conference of Data Protection and Privacy Commissioners Website <http://www.privacyconference2014.org/media/16427/Resolution-Big-Data.pdf>

6.1.2 「忘れられる権利」

欧州の新たなデータ保護の枠組みとなるEUデータ保護規則案において個人のデータの削除を求める「忘れられる権利」の在り方が議論になる中、2014年欧州司法裁判所がプライバシー保護の観点から検索企業に対して一定の条件下で検索結果の削除義務を認める裁定を下した。

2010年11月4日、欧州委員会は、個人データの新たな包括的枠組みを公表し、その中で「忘れられる権利」（Right to be Forgotten）の考え方が初めて掲げられた(1)。2012年1月には欧州委員会が1995年に採択されたEUデータ保護指令の包括的な改正に向けてEUデータ保護規則案を提案した(2)。同規則案では第17条として「忘れられる権利及び消去権」を規定し、データの当事者は、データが本来の処理目的において必要なくなった場合、本人が処理に対する同意を取り下げた場合、同意した保有期間を過ぎた場合、データの処理が同規則に従わない場合等に、データの管理者に対してデータの削除とデータの頒布の中止を実行させる権利があるとしている。一方、現行のEUデータ保護指令にも第12条(b)（データ消去権等）が規定されているが、データの当事者は、同指令に従わずに取り扱われたデータに対して、データの管理者に修正、消去、又はブロックを実施させる権利があるとするのみである。EUデータ保護規則案では、データの当事者がデータの消去を請求できる条件が明確化され、その権利も拡張されたといえる。その後、欧州司法裁判所の裁判事例（「海外の状況、技術動向、制度、規制」参照）を経て、2014年3月に欧州議会の第一読会で採択されたEUデータ保護規則案の修正案では、第17条の「忘れられる権利」の文言は削られ、単に「消去権」とされたが、実質的な権利の内容や対象は欧州委員会の原案より拡大された(3)。今後はEUの立法権を持つ欧州議会及び欧州理事会による修正協議が行われ、2015年内の規則成立後、2年間の委任法令（施行細則等）の制定期間を経て、2017年からの適用が有力視されている(4)。

2014年には、国内でも「忘れられる権利」に関連する司法判断が注目を浴びた。ヤフーが提供する検索サービスで自分の名前を検索すると、過去（2012年12月）の男性の逮捕に関する記述が表示されることが名誉毀損とプライバシーの侵害に当たるとして、男性がヤフーに対して検索結果の表示差止めと損害賠償等の支払を求めた訴訟において、2014年8月7日、京都地裁は男性の請求を棄却した。検索結果に表示されるのはリンク先の存在とURLで、逮捕事実の摘示を行っているものではないため名誉毀損の要件を満たさないとし、また、男性の逮捕事実が社会的な関心が高いものであり、判決時点で逮捕から1年半しか経過していないことから、検索結果の表示は公共の利害に関するもので、プライバシーの侵害にも当たらないとした(5)。

一方、Googleの検索サービスで自分の名前を検索すると、反社会的集団に関わった過去に関する検索結果が出てくるのはプライバシー侵害だとして日本人男性がGoogleの米国本社に検索結果の削除を求めた仮処分申請に対して2014年10月9日、東京地裁は男性の訴えを認め、男性が求めた237件のうち、著しい損害を与えるおそれがある122件について、検索結果の記事タイトルとその下に表示される検索語を含む抜粋（以下「スニペット」という。）の削除を命じる決定を出した。同年10月22日、Google日本法人が検索結果の削除に応じる方針を明らかにし、男性側も同日までに削除対象の大部分が表示されなくなっていることを確認した。(6)

同決定により、人格権を侵害する内容を含むコンテンツだけでなく、検索サービスによって

機械的に表示された検索結果やスニペットに関しても、人格権を侵害する内容が含まれる場合は検索結果の削除が認められるという裁判所の考え方が確立されつつあるとの見方もある(7)。

国内では「忘れられる権利」に対する法制化の動きはまだないものの、一部の民間事業者では独自に議論が始まっており、国内で最も利用者数の多い検索サービスを提供するヤフーは、2014年11月に外部の専門家からなる有識者会議を設置し、「表現の自由」や「知る権利」、プライバシーのバランスに配慮した、検索結果の削除に関する判断の在り方を検討している(8)。

●海外の状況、技術動向、制度、規制

■Google Spain及びGoogleに対する検索結果の削除命令

2010年、スペイン人男性が、男性の過去に関する新聞記事へのリンクが表示されるのはプライバシーの侵害だとして、新聞社とGoogle Spain及びGoogleに対して情報の削除を命令するよう申立てた訴訟に関して、2013年に公開された欧州司法裁判所のニーロ・ヤースキネン（Niilo Jääskinen）法務官（Advocate General）(9)の意見書では、現行のEUデータ保護指令から「忘れられる権利」が一般的な権利として導かれるものではなく、検索サービス事業者は同指令に基づき検索結果を削除する義務も負わない（検索サービス事業者はデータ保護指令のデータの管理者には当たらない）との見解が示された(10)。しかし、2014年5月、欧州司法裁判所はデータ保護指令の第12条(b)（データ消去権等）、第14条第1項(a)（データ処理の拒否権）の規定に従い、プライバシー保護の観点からGoogle等の検索サービス事業者は一定の条件下でリンクを削除する義務があるとする裁定を下した(11)。なお、同判決で認められたのは人名の検索に基づく検索結果であり、コンテンツ自体は削除されるものではない。判決を受け、同月Googleは欧州版Google検索での検索結果の削除をリクエストするフォームを公開した。ただし、対象はEU加盟国とアイスランド、ノルウェー、リヒテンシュタイン、スイスに限定されている。Googleは2015年2月12日の時点で、同フォームで約21.6万件のリクエストを受け取り、そのうち40.3%を削除したとしている(12)。

---

(1) European Commission,“European Commission sets out strategy to strengthen EU data protection rules (IP/10/1462),” November 4, 2010. <http://europa.eu/rapid/press-release_IP-10-1462_en.htm>
(2) European Commission,“Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012) 11 final),” January 25, 2012. <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC0011&from=en>
(3) 今岡直子「E1572-「忘れられる権利」と消去権をめぐるEU司法裁判所の裁定」『カレントアウェアネス-E』No.261, 2014.6.19. <http://current.ndl.go.jp/e1572>
(4) 電子情報技術産業協会「個人情報保護法への対応活動」『JEITAだより』vol.10, 2014.7.25, p.4. <http://www.jeita.or.jp/japanese/letter/pdf/vol10/2014_summer.pdf>
(5) 「時流・底流：忘れられる権利 日本とEU、司法判断に差」『毎日新聞』2014.9.8.
(6) 「グーグル検索結果の削除命令　記事タイトル・要約も対象　東京地裁、人格権に配慮」『日本経済新聞』2014.10.20;「グーグル　削除応じる　検索結果「裁判所の決定尊重」」『日本経済新聞』2014.10.23.
(7) 清水陽平「「忘れられる権利」のいま」『SYNODOS』2014.11.20. <http://synodos.jp/society/11698>
(8) 「検索結果とプライバシーに関する有識者会議」2014.11.7. ヤフーウェブサイト <http://publicpolicy.yahoo.co.jp/2014/11/0717.html>
(9) EU加盟国政府の合意によって任命され、公平・独立の立場から欧州司法裁判所が扱う案件に対する意見（裁判官に対する拘束力はない）を示す。
(10) Court of Justice of the European Union,“Advocate General Jääskinen considers that search engine service providers are not responsible, on the basis of the Data Protection Directive, for personal data appearing on web pages they process (Press Release No 77/13),” June 25, 2013. <http://europa.eu/rapid/press-release_CJE-13-77_en.htm>
(11) Court of Justice of the European Union,“Judgment of the Court (Grand Chamber),” May 13, 2014. <http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=en>
(12)「欧州のプライバシーに基づく検索結果の削除リクエスト」（2015年2月12日時点）Googleウェブサイト <https://www.google.com/transparencyreport/removals/europeprivacy/?hl=ja>

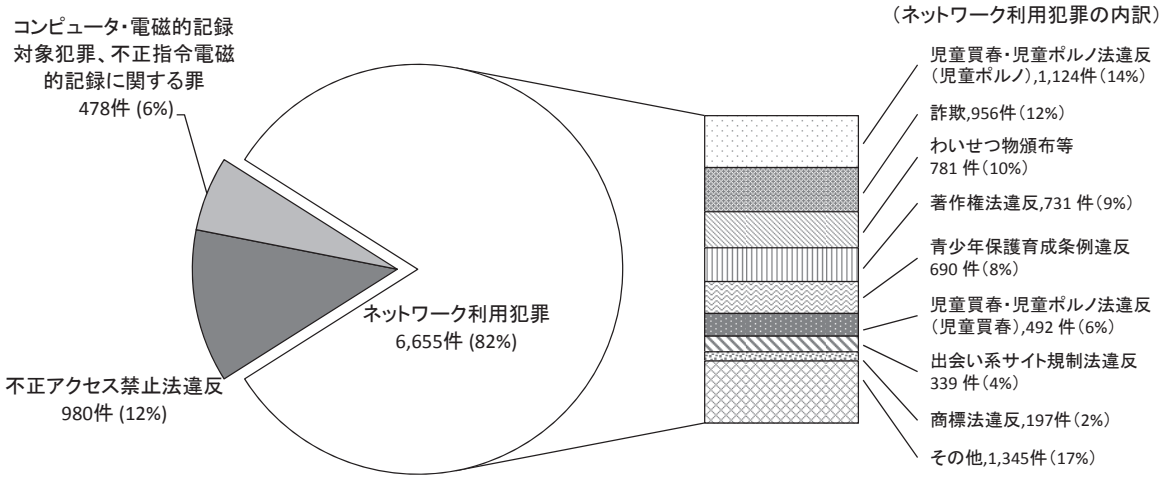
6.2　サイバー犯罪・トラブル

6.2.1　サイバー犯罪の発生状況

国内のサイバー犯罪の検挙件数、相談件数は年々増加傾向にある。サイバー犯罪の中では、ネットワーク利用犯罪（児童ポルノ、詐欺、わいせつ物頒布、著作権法違反、青少年保護育成条例違反、出会い系サイト規正法違反、商標法違反）が多くを占めている。

警察庁の発表によれば、2013年中のサイバー犯罪（用語集参照）の検挙件数は8,113件となり、過去最悪（前年度比10.6%増）を記録した。このうち、ネットワーク利用犯罪が6,655件（約82%）とサイバー犯罪の中で大多数を占めている。ネットワーク利用犯罪には、児童ポルノ、詐欺、わいせつ物頒布等、著作権法違反、青少年保護育成条例違反、児童買春等が含まれている。ネットワーク利用犯罪以外は、不正アクセス禁止法違反が980件（約12%）、コンピュータ・電磁的記録対象犯罪及び不正指令電磁的記録に関する罪が478件（約6%）である（図1参照）。ただし伸び率でみると、コンピュータ・電磁的記録対象犯罪及び不正指令電磁的記録に関する罪の増加が著しく、前年比168.5%増となっている。(1)

図1　2013年中のサイバー犯罪の罪名別割合



（出典）警察庁「平成25年中のサイバー犯罪の検挙状況等について」2014.3.27, p.1. <http://www.npa.go.jp/cyber/statics/h25/pdf01-2.pdf>を基に三菱総合研究所作成。

また、サイバー犯罪等に関する2013年中の相談件数は84,863件と前年比9.1%増であり、特に不正アクセス等、コンピュータ・ウイルスに関する相談は6,220件と前年比29.5%増で急増している(2)。なお、不正アクセス行為の発生状況に関する警察庁の発表によれば、2013年中の不正アクセス行為の認知件数は2,951件（前年比1,700件増）であり、そのうち検挙された件数は980件（前年比437件増）、検挙率は33.2%（前年43.4%）と過去最低となった（総論「情報通信技術の進展とサイバーセキュリティ」図2参照）。

近年、手口が悪質・巧妙化するとともに被害額も急激に増えているサイバー犯罪として、インターネットバンキングに係る不正送金事件がある（詳細は6.2.5 不正送金を参照）。また件数とし

て顕著な増加傾向にあるのが、著作権法違反である。典型的な事例は漫画のスキャンデータ、テレビ番組録画データ、DVDからのキャプチャ動画データ等を著作権者の承諾を受けることなく、インターネット上のサーバにアップロードし、利用者に配信するといった犯罪である。

サイバー犯罪（特にネットワーク利用犯罪）については、犯罪手段として用いられた技術を規制するのかあるいは、その開発者を罰する必要があるのか等が常に課題となる（事例研究参照）。

●事例研究

■Winny事件

P2P（Peer To Peer）型ファイル共有ソフトWinnyの開発者である金子勇東京大学特任助手（当時）が2004年に逮捕された事件である。Winnyを配布した行為が、Winnyを利用してなされた著作権侵害行為の幇助とみなされた。一審判決は有罪であったが、二審では無罪、2011年の最高裁判決(3)では検察側の上告を棄却し無罪が確定した。なお、Winnyを利用してゲームや映画をダウンロード可能な状態にしたとして逮捕された正犯（同特任助手とは面識のない第三者）による著作権侵害（公衆送信権侵害）自体は有罪が確定している。

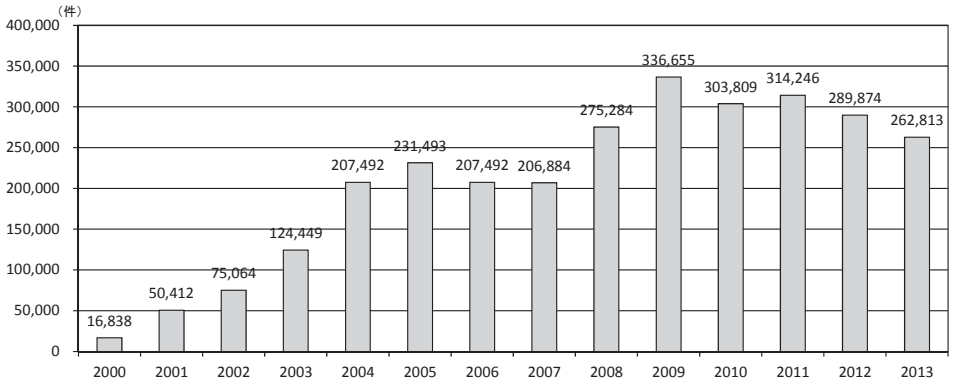
本事件に関しては、価値中立のソフトウェアの提供が著作権侵害行為幇助に当たるか否か、幇助する意図があったかなどが争点となった。

●海外の状況、技術動向、制度、規制

■Internet Crime Complaint Center（IC3）

2000年に設立されたInternet Crime Complaint Center（IC3）は、米国連邦捜査局（Federal Bureau of Investigation: FBI）と非営利団体National White Collar Crime Center（NW3C）が共同で運用している、サイバー犯罪の告発・届出窓口である。IC3に告発・届出されたサイバー犯罪は捜査のため法執行機関に転送される可能性があるため、告発・届出の際に虚偽の情報を提供すると、刑事罰に問われる場合がある。2013年にIC3が受理した告発・届出は合計262,813件（図2）、金銭被害は781百万ドルに達する（米国外からの届出を含む）。(4)

図2　IC3へのサイバー犯罪の届出件数の推移



（出典）Internet Crime Complaint Center,“2013 Internet Crime Report,”p.3. <http://www.ic3.gov/media/annualreport/2013_IC3Report.pdf>を基に三菱総合研究所作成。

(1)　警察庁「平成25年中のサイバー犯罪の検挙状況等について」2014.3.27, p.1. <http://www.npa.go.jp/cyber/statics/h25/pdf01-2.pdf>
(2)　同上, p.3.
(3)　最高裁判所第三小法廷平成23年12月19日判決
(4)　Internet Crime Complaint Center,“2013 Internet Crime Report,”p.3. <http://www.ic3.gov/media/annualreport/2013_IC3Report.pdf>

6.2.2　SNSの普及に伴う脅威

Facebook、Twitter、LINEなどのソーシャルネットワーキングサービス（SNS）が普及する中、SNSの便利な機能が犯罪に悪用されたり、ネットいじめやサイバーストーカーなどの嫌がらせ行為に使われる事例が増えている。

近年、全世界的にソーシャルネットワーキングサービス（SNS）の利用者が急激に増加している。米国の調査会社eMarketerによると、全世界のSNSユーザ数は2014年に18.2億人になり、今後2017年に23.3億人になると推計されている(1)。

平成25年通信利用動向調査によれば、国内のソーシャルメディア（SNSに代表されるインターネット上で相互のやり取りができる双方向のメディア）の利用率は全体で42.4%、年代別では6～12歳で15.9%、13～19歳で57.2%、20代の65.5%をピークに30代58.9%、40代43.5%、50代29.8%と幅広い世代にSNSが普及している状況がうかがえる(2)。

SNSが普及する一方、簡単にメッセージを送ったり、写真や投稿を友達同士で共有したり等、SNSの便利な機能が犯罪に悪用されたり、トラブルの原因となったりする事例が増えている。

若い世代において問題となっているケースの1つにSNS上のネットいじめがある。学校裏サイトなどネット上のいじめは以前からあるが、近年はSNS上で無視する、悪口を書くなどのいじめ行為が行われたり、SNS上の些細なトラブルがきっかけでいじめに発展してしまうこともある。閉じたグループ内で行われるやり取りが多いため外部に発覚しづらく、いじめがエスカレートした結果、暴行、殺人、自殺等の事件に発展してしまう事例も発生している(3)。

SNSによるストーカー行為（サイバーストーカー）の事例も増えている。相手が拒絶しているにもかかわらず、執拗にメッセージを送りつけるのが典型的な例であるが、こうした行為は「ストーカー行為等の規制等に関する法律」（いわゆる「ストーカー規制法」。平成12年法律第81号）の規制の対象となっておらず、対応が急がれている(4)。また、SNS上で公開されている写真や投稿を悪用して、相手の生活が探られる危険性もある。2012年に神奈川県逗子市で女性が元交際相手の男に刺殺された事件では、元交際相手の男が女性のFacebookの写真や書込みから住まいを特定しようとしていた(5)。近年では、元交際相手などの個人的な写真を嫌がらせ目的でインターネット上に拡散させる「リベンジポルノ」も深刻な社会問題となっている。リベンジポルノに関しては被害者が受ける影響の深刻さから法制化が急がれ、2014年11月「私事性的画像記録の提供等による被害の防止に関する法律」（いわゆる「リベンジポルノ防止法」。平成26年法律第126号）が施行された。同法ではSNSによる拡散も罰則の対象となる。

SNSの利用によって意図せずトラブルに巻き込まれる事例もある。2010年頃から徐々に注目を集めるようになったSNS上の「炎上事件」では、無断で撮影した他人の写真を公開したり、飲食店等で不適切な写真を投稿したり等、SNSの影響範囲を理解せずに利用することがトラブルの原因になっている(6)。

このような状況を受け、総務省では「国民のための情報セキュリティサイト」において一般利用者向け、企業・組織向け、子ども向けに分けてSNS利用上の注意点について啓発を行っている(7)。警察庁や、情報処理推進機構（IPA）も随時注意喚起を行うとともに啓発コンテンツを公開している。また、文部科学省では、SNSによるトラブルの実態などを踏まえ、教育現場で

の対策として、情報化社会の新たな問題を考えるための児童生徒向けの教材や教員向けの手引書を作成・公開している(8)。一方民間では、ソーシャルゲーム等の事業者が注意喚起や啓発コンテンツの提供等の取組を進め始めている(9)。

●事例研究

■アカウント乗っ取り

第三者にSNSのアカウントが不正にログインされ、アカウント内の情報を窃取されたり、勝手に投稿され、メッセージを送信されたりするなどのアカウント乗っ取りが多く発生している。無料通話アプリのSNS「LINE」では、何らかの方法で手に入れたメールアドレスとパスワードなどを使ってアカウントを乗っ取り他人になりすまして、メッセージを送りつけた相手に購入させたプリペイドカードの情報をだまし取る詐欺事件が続発している。これを受けてLINEでは、利用者に向けてほかのサービスと同じパスワードを使い回さないよう啓発するとともに、認証方法としてパスワードのほかに「PINコード」（追加の暗証番号）を使う二要素認証を利用できるようにシステムを改良している(10)。

●海外の状況、技術動向、制度、規制

■ロマンス詐欺

米国を始めとする海外では、SNSや交流サイトなどを通じて知り合った相手を騙して、恋人や婚約者のようにふるまって最終的に金銭を送金させる、一種の結婚詐欺とも言える「ロマンス詐欺（Online Dating Scams）」の被害が多発している。米国連邦捜査局（Federal Bureau of Investigation: FBI）が2013年に公表した資料によれば、犯罪者はSNS等で公開されている情報などをもとに、特定のターゲットを定め、相手の好みを推測した上で、偽のプロフィールや写真を使ってコンタクトしてくるとしており、典型的な手口を示して注意を呼びかけている。(11)

---

(1)　eMarketer, Inc.,“India Leads Worldwide Social Networking Growth,”November 19, 2013. <http://www.emarketer.com/Article/India-Leads-Worldwide-Social-Networking-Growth/1010396#ZLlF0JIMiomxKfrH.99>
(2)　「平成25年通信利用動向調査の結果（概要）」総務省ウェブサイト <http://www.soumu.go.jp/johotsusintokei/statistics/statistics05a/h25doukou.html>
(3)　「広島女子生徒殺害　元同級生に懲役13年　地裁判決」『日本経済新聞』2014.10.25;「県「フォローしていれば」熊本市・高1自殺　高校、情報共有せず「解決」と認識、悲劇再び」『西日本新聞』2014.10.23;「少女4人傷害容疑で逮捕　「LINE」のメッセージに仕返し」『読売新聞』（北九州版）2013.10.22.
(4)　ストーカー行為等の規制等の在り方に関する有識者検討会「ストーカー行為等の規制等の在り方に関する報告書」2014.8.5, pp.2-3. 警察庁ウェブサイト <https://www.npa.go.jp/safetylife/seianki/stalker/report/report.pdf>
(5)　「SNSの「友達」ひょう変　サイバーストーカー増殖　専門家「リスク知って」」『日本経済新聞』2013.4.2, 夕刊.
(6)　総務省編「第1部第4章第3節安心・安全なインターネット利用環境の構築」『平成26年版情報通信白書―ICT白書―』日経印刷, 2014, pp.291-292. <http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h26/pdf/26honpen.pdf>
(7)　「SNS利用上の注意点（一般利用者の対策）」国民のための情報セキュリティサイト <http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/enduser/security02/05.html>;「SNS利用上の注意点（企業・組織の対策）」国民のための情報セキュリティサイト <http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/staff/14.html>;「SNS（エスエヌエス）を使うときの注意」国民のための情報セキュリティサイトキッズ<http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/kids/sns/>
(8)　「情報化社会の新たな問題を考えるための児童生徒向けの教材、教員向けの手引書」文部科学省ウェブサイト <http://jouhouka.mext.go.jp/school/information_moral_manual/index.html>
(9)　総務省編「第1部第4章第3節安心・安全なインターネット利用環境の構築」前掲注(6), p.300.
(10)　LINE「他社サービスと同じパスワードを設定している皆様へパスワード変更のお願い」2014.6.12. <http://official-blog.line.me/ja/archives/1004331596.html>; LINE「重要 スマートフォン版LINEのセキュリティ強化のため、「PINコード」による本人確認手順を追加しました（7/17開始）」2014.7.15. <http://official-blog.line.me/ja/archives/1006009191.html>
(11)　Federal Bureau of Investigation,“Looking for Love? Beware of Online Dating Scams,”Feburuary 14, 2013. <http://www.fbi.gov/sandiego/press-releases/2013/looking-for-love-beware-of-online-dating-scams>

6.2.3　子どもとサイバー犯罪

スマートフォンや携帯ゲーム機を始めとするインターネットを利用できる携帯端末の普及により、子どもたちのインターネット利用がますます広まる中、子どもたちがサイバー犯罪の被害者や加害者になるケースが増えてきている。

スマートフォンやインターネット接続可能な携帯ゲーム機などの普及により、子どもたちがインターネットを利用できる環境が広がってきている。経済産業省の2013年の調査によれば、満10歳から満17歳までの青少年のうち、自分専用のパソコンを所有しているのは、デスクトップパソコンが3.8%、ノートパソコンが11.0%であるのに対し、スマートフォンは31.8%、携帯ゲーム機は69.1%、携帯音楽プレーヤーが37.9%となっている(1)。このような中、子どもたちがサイバー犯罪に巻き込まれるケースが増えてきている。例えば、子どもにも広く普及するSNS等が、一部出会い系サイトと同じ目的で利用されている実態があり、これに起因して児童・生徒が犯罪被害を受ける事例が発生している(2)。また、子どもが被害者になるケースだけでなく、SNSなどで特定の児童・生徒に対する誹謗・中傷を行う「ネットいじめ」の問題では、子どもが加害者になるケースもある。

このほかにも子どもたちに関係したサイバー犯罪には「児童ポルノ」がある。児童ポルノに関しては国際的に規制強化の動きがあり、2014年7月、日本国内でも「児童買春、児童ポルノに係る行為等の規制及び処罰並びに児童の保護等に関する法律」（いわゆる「児童ポルノ禁止法」。平成11年法律第52号）が改正され、個人が趣味で児童ポルノの写真や映像を持つ「単純所持」にも刑事罰が科せられることになった。その一方で、創作物への過度な規制等、表現の自由が脅かされる可能性を懸念する声もあり、漫画やアニメ、CGに関しては規制の対象から外れている(3)。

こうした状況の中、2009年4月から施行された「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」（いわゆる「青少年インターネット環境整備法」。平成20年法律第79号）では18歳以下の青少年がインターネットを利用する際は、保護者が利用を拒否する場合を除いてフィルタリングサービスの利用を義務付けている。また、現在では多くのパソコンやスマートフォンなどに「ペアレンタルコントロール」という監視機能が搭載されており、保護者の設定により子どもたちがゲームで遊んだり、インターネットにアクセスしたりする時間を制限したり、不適切なサイトにアクセスできなくしたりするなどの制御ができる。しかし、内閣府が満10歳から満17歳までの青少年3,000人を対象に実施した「平成25年度青少年のインターネット利用環境実態調査」によれば、携帯電話・スマートフォンを所有している青少年（59.5%）のうち、フィルタリングの利用率は55.2%で、前年度調査の63.5%から急激に低下しており、特にスマートフォンのフィルタリング利用率は47.5%に留まるなど、現状では制限が十分に機能しているとは言えない(4)。このような中、総務省では「国民のための情報セキュリティサイト」を通じて、保護者や子どもたち、それぞれに向けた啓発コンテンツを公開している(5)。また、青少年のインターネット利用の実態に関しては、内閣府や警察庁、総務省、経済産業省が様々な調査を実施、その結果を公開しているほか、警察庁では子どもたちと保護者に向けた啓発コンテンツ「キッズ・パトロール」を公開している(6)。一方、民間では、インターネット協会が「インターネットを利用する子どものためのルールとマナー集こどもばん」を公

開している(7)。また、学識経験者・学校関係者・保護者とで構成される専門家会議として、2008年に「子どもたちのインターネット利用について考える研究会（子どもネット研）」が設立されており、子どもの安全なインターネット利用に関して保護者に向けた教材「保護者のためのインターネットセーフティガイド」を公開するなどの活動を行っている(8)。

●事例研究

■LINEのID検索に対する年齢制限

無料通話アプリのIDを交換する掲示板（ID交換掲示板）(9)に起因する犯罪被害が増加している。LINEでは、2013年頃からID交換掲示板を出会い系サイトと同様の目的で利用されたことで、未成年が性犯罪に巻き込まれる事件が多発した。これを受け、LINEは2013年9月から18歳未満の利用者に対してLINEのID検索ができないような機能制限を実施した。18歳未満か否かの判別には、携帯電話事業者が利用者の登録情報に基づいて行う年齢判定機能を使用している。(10)

●海外の状況、技術動向、制度、規制

■米国におけるネットいじめ

米国でも「ネットいじめ」（Cyberbullying）は深刻な社会問題となっている。

ニューハンプシャー大学（University of New Hampshire）の研究チームが、10歳から17歳のインターネットユーザ約4,500人を対象にして、2000年・2005年・2010年に行った米国内の調査では、「オンラインでの嫌がらせ（Online Harassment）」を受けた割合は2000年の6%から2010年には11%に増加しており、被害者が女子である割合が2000年の48%から2010年には69%に増えている。特に、2010年の結果では、学校の友達や知り合いから、SNS上でいじめを受けるケースが増えているとしている。この背景として、女子については、オンライン環境で友達とコミュニケーションする機会が増えたことで、オフラインのいさかいがオンライン環境でも広がってしまう傾向にあると分析している(11)。

---

(1)　経済産業省「平成25年度我が国経済社会の情報化・サービス化に係る基盤整備（青少年インターネット利用環境整備に係る調査）機器ごとのインターネット利用状況調査報告書（委託先:ピットクルー）」2014.1, p.7. 経済産業省ウェブサイト <http://www.meti.go.jp/policy/it_policy/policy/pdf/H25_kikigoto.pdf>

(2)　警察庁「平成25年中の出会い系サイト及びコミュニティサイトに起因する事犯の現状と対策について」2014.2.27. <http://www.npa.go.jp/cyber/statics/h25/pdf02-2.pdf>

(3)　「児童ポルノ所持に罰則　改正法成立　アニメなどは対象外」『日本経済新聞』2014.6.18, 夕刊.

(4)　内閣府「平成25年度 青少年のインターネット利用環境実態調査 調査結果（概要）」2014.3, p.10. <http://www8.cao.go.jp/youth/youth-harm/chousa/h25/net-jittai/pdf/kekka_g.pdf>

(5)　「インターネット上のサービス利用時の脅威と対策」国民のための情報セキュリティサイト <http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/enduser/security02/index.html>; 国民のための情報セキュリティサイトキッズ <http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/kids/index.html>

(6)　「キッズ・パトロール」警察庁ウェブサイト <http://www.npa.go.jp/cyberpolice/kids/>

(7)　「インターネットを利用する子供のためのルールとマナー集こどもばん」2004.8.10. インターネット協会ウェブサイト <http://www.iajapan.org/rule/rule4child/v2/>

(8)　子どもたちのインターネット利用について考える研究会ウェブサイト <http://www.child-safenet.jp/>

(9)　LINE等の無料通話アプリのIDを交換する掲示板。IDだけでなく短文のメッセージや、居住地域、年齢、性別等の情報を公開し、それらの情報でユーザを検索できるものもある。

(10)「青少年保護のため18歳未満のユーザはLINE ID検索が利用できなくなります」2013.9.25. LINE公式ブログ <http://official-blog.line.me/ja/archives/21331557.html>

(11)　Lisa M. Jones et al.,“Online Harassment in Context: Trends From Three Youth Internet Safety Surveys (2000, 2005, 2010),”*Psychology of Violence*, vol.3 no.1, 2013, pp.53,64. <http://cola.unh.edu/sites/cola.unh.edu/files/research_publications/CV271.pdf>

6.2.4　ネット依存・スマホ依存

若い世代のインターネット依存、スマートフォン依存の傾向が顕在化しており、生活や学力への悪影響が懸念されている。同じくネット依存が社会問題化している韓国では、国を中心とした予防教育や治療体制等の整備が進んでいるが、我が国における対策は遅れている。

情報通信技術の進展に伴い、人々がインターネットやスマートフォンを使う機会が増加し、物心つく頃からインターネットやIT機器に慣れ親しんだ若い世代はデジタルネイティブとも呼ばれる。そのような状況の中、若い世代を中心にインターネットやスマートフォンを長時間利用し、生活や健康に支障をきたす、いわゆるネット依存、スマホ依存の問題が広がっている。

総務省が2014年に実施した「高校生のスマートフォン・アプリ利用とネット依存傾向に関する調査」（都立の全日制及び定時制の高等学校154校対象、有効回答数15,191票）によれば、高校生の4.6%が「ネット依存傾向高」群と判定されたという結果が出ている。依存傾向の高い生徒は、ネットのしすぎにより引きこもり気味になる、健康状態が悪化する、学校の遅刻や欠席が増えるなど日常生活へ悪影響を与えている割合が全体平均の4倍となっている。(1)

近年では、ソーシャルネットワーキングサービス（SNS）への依存傾向も強くなっている。スマートフォンによっていつでもどこでもSNSを利用できる環境になった一方で、常に友達の投稿やメッセージをチェックしていないと不安になるといった、SNSに縛られた生活に陥ってしまう危険性もある。前述の総務省調査における高校生のソーシャルメディア(2)利用状況に関する調査結果では、高校生でソーシャルメディアを利用しているのは全体の91.0%となり、男子（88.7%）より、女子（93.4%）の利用率が高い傾向にあった。利用するサービス別ではLINE（85.5%）、Twitter（66.9%）、Facebook（24.3%）の順に利用率が高くなっている。1日当たり平均利用時間では、LINE（80.9分）とTwitter（78.6分）の2つのサービスの利用時間が圧倒的に長く、男女別では女子の利用時間が長かった（LINE：96.7分、Twitter：95.0分）。特に、「ネット依存傾向高」群の生徒の場合、LINE（137.6分）、Twitter（171.0分）と各ソーシャルメディアを1日2時間以上利用している。また、全体平均と比べLINEとTwitterの利用時間の長さの傾向が逆転し、Twitterは全体平均の2倍以上の利用時間となっている(3)。

ネット依存、スマホ依存による学力への悪影響も懸念されている。文部科学省が小学校6年生及び中学校3年生を対象に毎年実施する全国学力・学習状況調査の2014年度の結果では、普段（月～金曜）、1日当たり1時間以上携帯電話やスマートフォンで通話やメール、インターネットをすると回答した児童・生徒の割合は小学校で約15%、中学校で約48%となった。いずれもこれらの時間が短い児童・生徒の方が全ての教科で平均正答率が高い傾向が見られた。(4)

ネット依存の問題は、日本だけでなく世界中で社会問題化している(5)。韓国では、2000年代からネット依存の相談窓口や専門の治療施設、治療プログラムを整備している。

文部科学省では、これら先行事例を参考に、2014年度からネット依存傾向の青少年を対象とした自然体験や宿泊体験プログラム「セルフチャレンジキャンプ」を開始し、国立青少年教育振興機構が事業を受託している。同機構の施設を利用した8泊9日のプログラムは認知行動療法、ネット依存学習、カウンセリング、自然体験活動等から構成されており、カウンセリングなどは国立病院機構久里浜医療センター（事例研究参照）が担当した。文部科学省では2016年

度までにキャンプの実施先を全国7か所まで拡大する方針としている(6)。

●事例研究

■ネット依存専門外来

国立病院機構久里浜医療センターは、2011年7月に国内初のネット依存治療研究部門及び専門外来を開設し、精神科医、臨床心理士、精神保健福祉士等の専門家が治療を開始している(7)。相談に来るのは中高生の親が多く、オンラインゲーム依存の相談内容が多いとしている(8)。

現在ネット依存に対して確立した治療法はないが、同センターでは患者の症状、発達背景、性格傾向、合併精神疾患、家族背景等の評価を基に、個々のケースの臨床的特徴を明らかにし、動機づけ面接と認知行動療法をベースにカウンセリングを加えた治療方針を決定している(9)。

●海外の状況、技術動向、制度、規制

■韓国のネット依存対策

日本以上にインターネット環境が普及している韓国では、2000年代からネット依存が社会問題化している。韓国では、情報社会振興院がインターネットの適正な利用を啓発する目的で韓国インターネット依存症センター（Korea Internet Addiction Center）を2002年に設立し、全国11か所に支部を設置している。同センターではカウンセリングや、各種キャンペーン、ネット依存の実態調査を実施するとともにネット依存対策に携わる人材育成にも力を入れている(10)。

また、韓国政府は、毎年小学4年生、中学1年生、高校1年生を対象に独自の「インターネット中毒自己評価スケール」に基づきネット依存の調査を実施している。同調査でネット依存のリスクが高いとされた子どもには、ネットと断絶された環境で11泊12日の集団生活を送る「レスキューキャンプ」等の治療を行っている。さらに、2011年から、午前0時から6時までの深夜時間に、16歳未満の青少年がオンラインゲームにアクセスできない「青少年夜間ゲームシャットダウン制」が導入され、2012年から18歳未満の青少年のオンラインゲーム利用時間を保護者が管理する「ゲーム時間選択制」が導入されている。(11)

このほか、ソウル市では24歳以下の若者のネット依存の予防及び治療を行う“I Will Center”を市内6か所に設置し、カウンセリングやネット依存の予防教育や普及啓発を行っている(12)。

---

(1)　総務省情報通信政策研究所「高校生のスマートフォン・アプリ利用とネット依存傾向に関する調査報告書」2014.7, pp.4, 15. <http://www.soumu.go.jp/main_content/000302914.pdf>
(2)　インターネット上で利用者同士、相互のやり取りができる双方向のメディアであり、SNSもその1つ。
(3)　総務省情報通信政策研究所　前掲注(1), pp.21, 23.
(4)　文部科学省国立教育政策研究所「平成26年度 全国学力・学習状況調査　調査結果のポイント」2014.8, pp.53-54. <https://www.nier.go.jp/14chousakekkahoukoku/hilights.pdf>
(5)　三原聡子ほか「ネット依存その2：諸外国における現状と予防教育」（第259回アルコール関連問題予防研究会演題概要）2014.4.17. <http://al-yobouken.com/pdf/H26/PREVENTION_NO259.pdf>
(6)　「「ネット依存」キャンプで克服―中1から大学生10人参加　行動を記録　関心の対象広く（学ぶ）―」『日本経済新聞』2014.10.17, 夕刊.
(7)　「ネット依存治療部門（TIAR）」国立病院機構久里浜医療センターウェブサイト <http://www.kurihama-med.jp/tiar/index.html>
(8)　「特集ワイド：推計500万人、ネット依存の「治療」　リアル人間関係が鍵」『毎日新聞』2012.11.13, 夕刊.
(9)　三原聡子ほか「インターネット依存に関するわが国の現状」2012.4.3. <http://www.kurihama-med.jp/tiar/pdf/20120403_no1_workshop_report1.pdf>
(10)　“About Center.”Korea Internet Addiction Center Website <https://www.iapc.or.kr/english/aboutcenter/GreetingsDirector.do>
(11)　河崎貴一「「ネット依存症」現状と対策―「日本と韓国」急増するネット依存者の実態―」『ヘルシスト』222, 2013.11.10, pp.23-24. <http://www.yakult.co.jp/healthist/222/img/pdf/p20_25.pdf>
(12)　“Introduction to I Will Center.”I Will Center Website <http://www.iwill.or.kr/>

6.2.5　不正送金

近年インターネットバンキングにおける不正送金事件が急増し、被害が拡大している。こうした中、金融機関はセキュリティ向上のために様々な取組を行っている。

全国銀行協会の2012年の調査（アンケート調査会社のモニター会員を対象にしたインターネット調査）によれば、インターネットバンキングの利用率は65.2%まで普及している。また、利用頻度は銀行内のATMに次いでおり、コンビニエンスストアやスーパーなどにあるATMと同程度に高い利用頻度となっている(1)。一方、警察庁の発表によれば2014年上半期のインターネットバンキングに係る不正送金事犯の被害件数は1,254件（2013年上半期217件）、被害額は約18億5200万円（2013年上半期は約2億1300万円）と急増した(2)。なお、警察庁は同期間中、不正送金事犯69事件で133人を検挙し、その6割以上が中国人であった(3)。被害の特徴としては、法人口座の被害が増えており、取扱金額の大きい法人口座を狙い、意識の低い企業が標的にされている可能性があるという(4)。こうした状況を受け、全国銀行協会では法人向けインターネットバンキングにおける不正送金に関して、利用者に注意を呼びかけている(5)。

不正送金はインターネットバンキングで使用される利用者のIDやパスワードなどの認証情報を盗用することで行われる。認証情報の入手方法としては、金融機関を騙った電子メールで偽の金融機関サイトに誘導し、そこで認証情報を入力させる、従来からある「フィッシング」のほか、何らかの経路で感染したマルウェアが、ユーザがインターネットバンキングへアクセスしたのを検知し、偽の認証画面を表示し、認証情報入力と同時に自動的に犯罪者の口座等に送金を行わせる高度な攻撃もある。

このような中、金融機関、信販会社、セキュリティベンダ等の会員で構成されるフィッシング対策協議会は「インターネットバンキングの不正送金にあわないためのガイドライン」を公開している。このガイドラインでは、利用者に向けて、認証に用いられる乱数表等（ID、パスワードに追加する認証要素）の入力を慎重に行い、パソコンを始めとする利用機器を最新の状態に保つといった基本的な対策について、チェックリスト等を示すことで啓発している。(6)

一方、各銀行も対策を講じている。銀行のホームページで利用者に向けた注意喚起や啓発が行われているほか、銀行の中には、利用者に送信される正規の電子メールに電子署名を付けているケースもある。このような各銀行が行っているセキュリティへの取組はそれぞれのホームページで紹介されている。

また、不正送金対策として効果的な本人認証の強化策の例としては、ログインに際して単純なIDとパスワードの組合せだけでなく、携帯電話やスマートフォンに送信される、又はトークン（パスワード表示専用端末）に表示される、「ワンタイムパスワード」と呼ばれる「使い捨て」のパスワードを必要とする仕組みや、パスワードの入力を一定回数以上間違えると自動的にロックされる仕組みなどがある。また、利用者が使っているパソコンやネットワークの環境を解析することで、普段とは異なる環境からのアクセスがあった場合に、ログインを遮断するなどの対策をとっている銀行もある。ほかにも、キーボードへの入力内容を窃取するマルウェアである「キーロガー」対策として、パソコンの画面に表示したキーボードからマウス等でパスワードなどを入力させる「ソフトウェアキーボード」を導入しているケースもある。

さらに、不正送金を含むサイバー攻撃全般に対応するために、金融機関同士の情報共有と連携を目的とした組織「金融ISAC」が2014年8月に設立されている。金融ISACは、金融分野で広がるフィッシング被害、不正送金被害、APT攻撃、DDoS攻撃、脆弱性・ゼロデイ攻撃の脅威などのサイバーセキュリティに関する情報を、金融機関の間で共有し、相互に連携して対策にあたる枠組みである。(7)

●事例研究

■FISC（金融情報システムセンター）によるガイドライン

金融庁所管の金融情報システムセンター（FISC）では、金融情報システムの安全性確保や金融業務の安定的遂行のための自主基準を策定しており、金融機関や金融機関に情報システムを提供するメーカー等で広く利用されている。「金融機関等コンピュータシステムの安全対策基準」は金融情報システムに関する安全対策の共通の指針であり、2011年に発刊された第8版及び2013年改訂の第8版追補が最新版である。そのほか、金融機関におけるBCP策定・見直しに関する「金融機関等におけるコンティンジェンシープラン策定のための手引書」（2013年改訂）、金融機関等のシステム監査導入と推進に関する「金融機関等のシステム監査指針」（2014年改訂）、金融機関におけるセキュリティポリシーの策定に関する「金融機関等におけるセキュリティポリシー策定のための手引書」（2008年改訂）等が発刊されている。(8)

●海外の状況、技術動向、制度、規制

■Financial Services Information Sharing and Analysis Center（FS-ISAC）

米国では1998年に重要インフラ各分野に対してセキュリティ情報を共有・分析するための組織であるISAC（Information Sharing and Analysis Center,「アイザック」と読む。）の設立が促されたことを受け、1999年10月に、財務省の所管で銀行・金融分野のISACとしてFinancial Services Information Sharing and Analysis Center（FS-ISAC）が設立された。会員企業は銀行、証券会社、保険会社などで、2014年8月の時点で加盟企業は4,600社を超えている。FS-ISACは財務省及び金融分野調整協議会（Financial Services Sector Coordinating Council: FSSCC）と連携して、金融分野の脅威への対応、分野内の情報共有を主導するほか、金融分野における独自のサイバー演習も実施している(9)。また、2014年に設立された日本の金融ISACは今後FS-ISACとも連携し、情報共有を図るとしている(10)。

(1)　全国銀行協会「よりよい銀行づくりのためのアンケート結果について（2012年度）」2012.12.28, p.63. <http://www.zenginkyo.or.jp/news/2012/12/28150000.html>
(2)　警察庁「平成26年上半期のインターネットバンキングに係る不正送金事犯の発生状況について」2014.9.4, pp.1-2. <https://www.npa.go.jp/cyber/pdf/H260904_banking.pdf>
(3)　同上, p.1.
(4)　「不正送金被害18億円、ネットバンキング、地銀標的目立つ、今年上半期」『日本経済新聞』2014.9.4, 夕刊.
(5)　「法人向けインターネット・バンキングにおける不正送金にご注意！」全国銀行協会ウェブサイト <http://www.zenginkyo.or.jp/topic/sagijiken_ib_co/index.html>
(6)　フィッシング対策協議会 ガイドライン策定ワーキンググループ「インターネットバンキングの不正送金にあわないためのガイドライン」2014.5.12, pp.5-6. <https://www.antiphishing.jp/report/pdf/internetbanking_guideline.pdf>
(7)　金融ISAC「一般社団法人 金融ISACの設立について―高度化するサイバー攻撃対策のため金融機関間の情報共有を促進―」2014.8.7. <http://www.f-isac.jp/press_release/20140807.html>
(8)　吉田晃憲「金融機関のセキュリティ対策の動向について」2007.2.14, pp.6, 8, 11. <https://www.jpcert.or.jp/present/2007/ciip2007_06.pdf>
(9)　三菱総合研究所「米国のセキュリティ情報共有組織(ISAC)の状況と運用実態に関する調査（平成21年度内閣官房情報セキュリティセンター委託調査）」2010.3, pp.102-105. <http://www.nisc.go.jp/inquiry/pdf/fy21-isac.pdf>
(10)　金融ISAC　前掲注(7)

6.2.6　電子商取引にかかわるトラブル

インターネットを活用した消費者向け電子商取引が年々拡大する一方で、様々な問題が発生している。経済産業省では、これらの問題に対して適用される民法等の法律を明らかにする準則を定めている。消費者庁においても景品表示法上のトラブルなどに対してガイドラインを示している。また、海外の事業者からの越境電子商取引の拡大に伴い、トラブルが増加している。

経済産業省が発表した2013年の日本における消費者向け電子商取引（EC）市場規模は11.2兆円（前年比17.4%増）、企業間電子商取引の市場規模については、狭義で186兆円（前年比4.4%増）に、広義では269兆円（前年比2.8%増）に拡大している(1)。

手軽にネットショッピングやネットオークションを利用できるようになった一方で、これらにかかわるトラブルが増えている。国民生活センターに寄せられたインターネット通販全体に関する相談件数は、2014年12月31日時点で168,917件と、前年同期（133,594件）に比して急激に増加している(2)。

経済産業省では、電子商取引、情報財取引等において発生する法的問題点について、民法等の法律がどのように適用されるのかを明らかにし、取引当事者間のトラブルを未然に減らし、取引を円滑化することを目的として「電子商取引及び情報財取引等に関する準則」を定めている。市場の要請等に応じて、ほぼ毎年、準則の見直しを行っている。近年の裁判例では、電子商店街（ネットショッピングモール、以下「モール」という。）に出店する店舗の商標権侵害に対して、一定の要件を満たす場合、モール運営者も責任が問われるとの一般論が示されており、準則では、利用者の個別の店舗との取引によって生じた損害について、モール運営者は原則として責任を負わないとしつつも、利用者がモールの運営者を売主と誤認するような状況が作られていた場合、運営者が責任を負う場合があり得るとし、注意を促している。(3)

消費者庁では、「不当景品類及び不当表示防止法」（いわゆる「景品表示法」。昭和37年法律第134号）上の問題として、「いわゆるフリーミアム（基本的なサービスを無料で提供し、高度な、あるいは、追加的なサービスを有料で提供して収益を得るビジネスモデル）における正確でない「無料」といった表示」、「目立たない箇所に断片的に「事実」を記載しているとしても、全体として消費者に誤解を与え得るような表示」を挙げている。例えば、口コミサイトにおけるサクラ記事、広告主から報酬を得ていることが明示されない書込み等、一般消費者に誤認される表示について、景品表示法に違反する表示が行われないようガイドラインを示している(4)。

2013年度の日本の消費者による米国及び中国事業者からの越境電子商取引（以下「越境EC」という。）の購入額は1915億円となり、年々増加している。また、米国及び中国の消費者の日本の事業者からの越境ECによる購入額はそれぞれ4323億円、3902億円となっており、日本の消費者による購入額と同様に増加している(5)。越境EC市場拡大に伴い、商品の製品規格などが自国の規格と合致しなかった、購入した商品が不良品・偽物であった、等のトラブルも起きている(6)。また、越境ECでは、企業やサーバが日本国内にある場合や契約に適用される法律が明記されている場合でも、消費者保護の観点から消費者が居住する国の法律が適用される可能性が高いため、越境ECを行う企業は注意が必要である。海外の消費者が購入した商品によって、負傷したり病気になったりした場合、日本国内の事業者は消費者が居住する外国の法律に基づき製造物責任を問われることになる(7)。

●事例研究

■電子商取引（EC）の不当表示等に関するガイドライン

消費者庁では、景品表示法上で問題となる事項や事業者に対して守るべきガイドラインである「インターネット消費者取引に係る広告表示に関する景品表示法上の問題点及び留意事項」を2011年10月に発表している。この中で口コミサイトについては、商品やサービスを提供する事業者が、自らあるいは第三者に依頼して口コミ情報を掲載し、それが実際の商品やサービスよりも有利であると誤認されるものである場合は、景品表示法上の不当表示として問題となるとしていた。2012年のガイドラインの改訂では、ステルスマーケティングの手法について「問題となる事例」を追加し、商品やサービスを提供する事業者が、口コミ投稿の代行を行う事業者に依頼して口コミを多数書き込ませて評価を変動させ、あたかも一般消費者の多数から好意的評価を受けているかのように表示させることを、問題として挙げている。ただし、具体的な表示が景品表示法に違反するか否かは、個々の事案ごとに判断されるとしている。(8)

●海外の状況、技術動向、制度、規制

■越境電子商取引でのトラブル

海外事業者が運営するサイトを利用した電子商取引でのトラブル事例を消費者庁越境消費者センター（Cross-Border Consumer Center Japan: CCJ）がまとめている。CCJでは海外ショッピング（インターネット・店頭取引を含む）に関するトラブル相談を受け付けている。模倣品が届いたり、商品が届かなかったり、事業者と連絡が取れなくなったり等、詐欺の疑いがある悪質な通販サイトに関する相談件数は年々増加しており2013年には年間2,600件を超えている(9)。

消費者庁は、未然防止と被害拡大防止を目的として、模倣品を販売するウェブサイトや詐欺が疑われるウェブサイトをまとめた「悪質な海外ウェブサイト一覧」を公開している。過去に相談を受けたサイト等から作成したものであり、網羅したものではない。リストに掲載されていないウェブサイトであっても悪質なウェブサイトには、①正確な運営情報（運営者氏名・住所・電話番号）が記載されていない、②正規販売店の販売価格よりも極端に値引きされている、③日本語の表現が不自然である、④支払い方法が銀行振込のみとなっており、クレジットカードが利用できない、というような特徴が見られることから注意が必要とされている(10)。

---

(1)　経済産業省商務情報政策局情報経済課「平成25年度我が国経済社会の情報化・サービス化に係る基盤整備（電子商取引に関する市場調査）報告書」2014.8.26, pp.5-6. <http://www.meti.go.jp/press/2014/08/20140826001/20140826001-4.pdf>
(2)　「インターネット通販」国民生活センターウェブサイト <http://www.kokusen.go.jp/soudan_topics/data/internet2.html>
(3)　経済産業省「電子商取引及び情報財取引等に関する準則」2014.8. <http://www.meti.go.jp/press/2014/08/20140808003/20140808003-3.pdf>
(4)　消費者庁「インターネット消費者取引に係る広告表示に関する景品表示法上の問題点及び留意事項」2012.5.9. <http://www.caa.go.jp/representation/keihyo/files/3/koukoku.pdf>
(5)　経済産業省商務情報政策局情報経済課　前掲注(1), p.7.
(6)　同上, pp.148-149.
(7)　経済産業省「国境を越える電子商取引の法的問題に関する検討会報告書」2010.9, pp.27-30. <http://www.meti.go.jp/policy/it_policy/ec/cbec/cbec_images/crossborderec_houkokusho.pdf>
(8)　消費者庁「「インターネット消費者取引に係る広告表示に関する景品表示法上の問題点及び留意事項」の公表について」2011.10.28, pp.1-2. <http://www.caa.go.jp/representation/pdf/111028premiums_1_1.pdf>
(9)　「悪質な通販サイトに関するトラブルの実態」消費者庁越境消費者センターウェブサイト <http://www.cb-ccj.caa.go.jp/counterfeit/index.html>
(10)　消費者庁「悪質な海外ウェブサイト一覧」2014.10.10. <http://www.caa.go.jp/adjustments/pdf/141010adjustments_1.pdf>

6.2.7　電子マネーのリスク

事業者が独自に発行した電子マネーが決済サービスで使われるようになっている。一方、利用者にとっては、電子マネーを発行する運営会社が破綻すると現金から交換した電子マネーの価値がなくなったり、アカウントの乗っ取りにより不正に利用されるなどのリスクもある。

電子マネーとは、現金同様の金銭的な価値を有する電子データであり、発行者が提供する決済システムを意味しており、小額決済に利用されている。発行者が価値を担保する電子マネーには、前払いした金額分を利用できるプリペイド型、クレジットカードと同様に利用者の信用に基づき後払いで利用できるポストペイ型に大きく分けられる。プリペイド型電子マネーには、交通系の代表であるSuicaやコンビニやスーパー等での利用される流通系のnanaco、WAONなどがあり、これらの月額利用料は、世帯平均で1万円を超えており普及が進んでいる(1)。また、カードを発行しないサーバ型は一般的にプリペイド型であり、店舗で購入したカードに書かれた番号を入力することでチャージ（入金）できる。オンラインゲームなどのインターネットでの決済に利用されている(2)。

プリペイド型電子マネーは「資金決済に関する法律」（平成21年法律第59号）により商品券等と同等に規制されており、発行者が発行額の1/2を供託金として引当てしており、比較的安全に運用されている。しかしながら、店舗の店員等が不正にチャージを行う事件やSNS等のアカウントを乗っ取り、本人になりすまして、サーバ型電子マネーにチャージさせる詐欺事件、アカウントを乗っ取り貯まっていたポイントを金品に交換する事件も発生している。

表1　電子マネーの種別

種別	概要	主な電子マネー
プリペイド型	あらかじめ入金した金額の範囲内で利用できる。	交通系、流通系、Edy
ポストペイ型	クレジットカード会社が発行しており、サインレスでクレジット決済と同様に利用できる。	VISA Touch、QUICPay、iD
サーバ型	基本的にプリペイド型であるが、カードは発行されず、主にインターネットでの決済に利用される。	WebMoney、BitCash
分散型	価値を担保する特定の発行者がおらず、各利用者が保持するデータ全体で価値が担保される。	BitCoin
ポイント型	利用額に応じてポイントとして還元される。貯まったポイントを現金と同様に利用することができるが、おまけであり、電子マネーには含めない場合もある。	Tポイント、楽天ポイント

（出典）各種資料を基に三菱総合研究所作成。

2009年に登場したビットコイン（Bitcoin）は分散型仮想通貨であり、インターネットでの決済手段として低コストで利用できる電子マネーとして注目されている。企業が発行する電子マネーは全ての決済情報はサーバに蓄積され管理されるが、分散型には発行主体が存在せず、P2P（Peer To Peer,「ピアトゥピア、ピーツーピー」と読む。）型の電子マネーであり、参加者全員の記録によって、決済情報の正しさを担保する仕組みとなっている。供託金等で担保した電子マネーではないため、運営会社が破綻した場合には保証がない。また、運営会社が自由に発行できるため、既に発行されている分の価値が下落することになる。

Bitcoinは、約1370万BTC（2015年1月1日時点[3]、通貨単位であるビットコインをBTCと記述する）が流通している。1BTCは約310米ドル（2015年1月1日時点[4]、円換算約36,000円[5]）で取引されており、時価総額約42億ドル（約4900億円）が流通していることになる。流通や利用が拡大するにつれてBitcoinの法的な規制が検討されるようになり、各国の金融当局がマネーロンダリング（資金洗浄）防止や消費者保護のために規制する方向で進んでいる。日本では、民法で規定する「通貨」、金融商品取引法で定める「有価証券等の取引」ともに「該当しない」とされた[6]。米国ニューヨーク州金融サービス局（DFS）はビットコイン取引会社に対する規制案として、一定水準の資本の保有や、「ビットライセンス」の取得、マネーロンダリング防止関連規則の遵守、サイバーセキュリティプログラムの維持、コンプライアンス担当者の採用、顧客の詳細情報の検証などの義務付けを示した。

●事例研究

■電子マネーの不正利用

クレジットカードの情報を登録することでオートチャージ機能を持つモバイルSuicaに対して、盗難やスキミングしたクレジットカードの情報を登録することで、クレジットカード所有者に対して課金される被害が発生している。また、サーバ型やポイント型のアカウントを乗っ取ることにより、Tポイントや楽天等のポイント、クレジットカードなど貯まっていたポイントが不正に換金性の高い金品に交換される被害が発生している[7]。

加えて、駅員や店員による不正な操作によりチャージする事件等運営者にとってリスクのある事件が発生している。

●海外の状況、技術動向、制度、規制

■ビットコインの不正引出し

分散型仮想通貨であるBitcoinには、現金とBitcoinを時価である評価額に応じて独自に交換しているビットコイン交換所が複数存在する。不正な取引情報を流すことで交換所が持つBitcoinが不正に支払われる可能性があるというセキュリティ上のリスクが指摘されていた。不正なトランザクションデータを何度も再送する取引展性（Transaction Malleability）と呼ばれるサイバー攻撃を受けてマウントゴックス（Mt.Gox）が保有する85万BTC（当時の交換レートで約490億円）に相当するBitcoinが流出した[8]。取引所を運営するMt.Goxは日本で破産手続が行われた。被害者による集団訴訟が発生している。

---

(1)　総務省統計局「家計消費状況調査年報（平成25年）結果の概況」2013, p.17. <http://www.stat.go.jp/data/joukyou/2013ar/gaikyou/pdf/gk03.pdf>
(2)　経済産業省商務情報政策局商務流通グループ取引信用課「商取引の支払に関する論点の中間整理（電子流通等を促進する支払手段に関する検討会）」2008.9.11, pp.9-15. <http://www.meti.go.jp/report/downloadfiles/g80911a02j.pdf>
(3)　「市場に出回っているビットコイン数の合計」Blockchainウェブサイト <https://blockchain.info/ja/charts/total-bitcoins>
(4)　「BTC/USD過去のデータ」Investing.comウェブサイト<http://jp.investing.com/currencies/btc-usd-historical-data>
(5)　日本円への換算は、日本銀行基準外国為替相場及び裁定外国為替相場（2015年1月中において適用）に基づき計算：1ドルについて本邦通貨116円。
(6)　「参議院議員大久保勉君提出ビットコインに関する質問に対する答弁書」（平成26年3月7日内閣参質186第28号）2014.3.7. 参議院ウェブサイト <http://www.sangiin.go.jp/japanese/joho1/kousei/syuisyo/186/touh/t186028.htm>
(7)　「Tサイトへの不正ログインによるなりすまし被害のご報告およびパスワード変更のお願い」2013.4.5. カルチュア・コンビニエンス・クラブウェブサイト <http://tsite.jp/r/information/web/index.html>
(8)　「動かないコンピュータ　ビットコイン取引所「Mt.Gox」」『日経コンピュータ』856号, 2014.3.20, pp.58-60.

主要事項執筆者一覧

執筆者所属：三菱総合研究所

執筆者	主要事項
情報通信政策研究本部主席研究員　村野（むらの）　正泰（まさやす）	1.3.1, 4.1, 4.2, 4.3, 4.4, 4.6, 5.1.1, 5.1.2, 5.1.3, 5.2.1, 5.2.2, 5.2.3, 5.2.4, 5.3.1, 5.3.2, 6.2.1
情報通信政策研究本部主席研究員　澤部（さわべ）　直太（なおた）	1.3.2, 1.3.3, 1.3.4
情報通信政策研究本部主任研究員　谷田部（やたべ）　智之（ともゆき）	1.1, 1.2.1, 1.2.3, 1.2.4, 1.3.6, 2.4, 6.2.6, 6.2.7
情報通信政策研究本部主任研究員　清水（しみず）　友晴（ともはる）	6.1.1
情報通信政策研究本部研究員　松本（まつもと）　尭（たかし）	1.2.5, 2.1, 2.2, 2.3, 3.1, 3.2, 3.3, 4.5
情報通信政策研究本部研究員　丸田（まるた）　佳織（かおり）	1.2.2, 1.3.5, 5.1.4, 5.2.5, 5.2.6, 6.1.2, 6.2.2, 6.2.3, 6.2.4, 6.2.5, 7.1, 7.2, 7.3

＊ 本稿におけるインターネット情報の最終アクセス日は、原則として、2015年1月13日である。