情報通信技術の進展とサイバーセキュリティ

要　旨

情報通信技術の進展は我々の生活を豊かにする一方、多くの社会的な問題を惹起しており、その主要なものがサイバーセキュリティの問題である。歴史的には、サイバーセキュリティの要素技術である暗号技術は、情報通信技術が進展する遥か前から軍事技術の一つとして、数千年にわたり利用され発展してきた。第二次世界大戦中に発達し、又は開発された無線通信、機械式暗号装置、コンピュータは、現在のサイバーセキュリティにつながる技術的基礎となった。第二次世界大戦後、コンピュータの商用利用の進展に伴い、先行的にコンピュータの利用を始めた金融部門などの民間における情報セキュリティの確保が課題となってきた。Webの開発と1995年のWindows 95発売を契機として、個人のPC利用とインターネット利用が広がり、サイバーセキュリティの確保は国家安全保障、個人のプライバシーの確保、青少年の健全な育成などを包含する大きな課題となってきている。

I　サイバーセキュリティと情報セキュリティ

20世紀に登場した情報通信技術（Information and Communication Technology: ICT, コンピュータ技術及びコンピュータと統合された通信技術）は、人類の発明の中でも重要なものの一つであり、我々の生活を大きく変化させてきた。だが、情報通信技術の進展は、一方では社会的な問題を惹起しており、その主要なものがサイバーセキュリティの問題である。

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）によれば、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」と定義されている。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(1)。

サイバーセキュリティと似た用語として情報セキュリティがある。国際標準（ISO/IEC 27000:2013（JIS Q 27001:2014））によれば、情報セキュリティは「情報の機密性、完全性及び可用性を維持すること」と定義されているとおり、情報通信技術を用いない情報（紙に記載された情報等）を含む一方で、サイバーセキュリティは「情報システム及び情報通信ネットワークの安全性の確保」といった観点をより強く謳っている。

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）に設置された情報セキュリティ政策会議がこれまでに決定してきた「情報セキュリティ基本計画」及び「国民を守る情報

＊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。

(1)　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。

セキュリティ戦略」の後継として2013年に決定した「サイバーセキュリティ戦略」では、名称を「情報セキュリティ」から「サイバーセキュリティ」に変更した理由を「従来の「情報セキュリティ」確保のための取組はもとより、広くサイバー空間に係る取組を推進する必要性と取組姿勢を明確化するため、本戦略の名称は「サイバーセキュリティ戦略」とした」(2)と述べている。

本報告書においても、「サイバーセキュリティ戦略」の考えを踏襲し、「情報セキュリティ」を包含する概念として「サイバーセキュリティ」をとらえ、「情報セキュリティ」が固有名詞的に用いられる場合を除き「サイバーセキュリティ」を用いる(3)。

Ⅱ　サイバーセキュリティの動向

情報通信技術の進展に伴い、インターネットは世界の隅々にまで張り巡らされ、国民の生活や社会活動、企業の経済活動、政府の行政活動に深く浸透してきている。インターネットが身近で不可欠なインフラとして利用されるようになるに伴い、様々な事件や問題も多く発生している。

近年においては、高齢者や青少年が情報通信技術を活用することで、サイバー犯罪事件の被害者、場合によっては加害者になるケースが広く見受けられる。

また、「モノのインターネット（Internet of Things: IoT）」と呼ばれるように、従来のPCなどだけではなく、様々な「モノ」（センサ、制御機器を組み込んだもの）がインターネットを介してモニターされ、コントロールされるようになってきている。「モノ」が外部から攻撃され不正に制御されることで、様々な事故や障害が発生する危険性が高まっている。

1　高度化するサイバー攻撃

2000年頃までのサイバー攻撃は、愉快犯的にコンピュータウイルス（以下「ウイルス」という。）を無差別に感染させ、あるいは不正アクセスにより企業や政府のウェブサイトを書き換えるようなものであったが、近年は金銭や情報の窃取や重要インフラの麻痺などを目的として、特定の組織を狙った高度で継続的な攻撃が行われることが多くなってきた。

近年発生した主なサイバー攻撃事件には表1に示すようなものがある。

(2)　情報セキュリティ政策会議「サイバーセキュリティ戦略」2013.6.10, p.3. <http://www.nisc.go.jp/active/kihon/pdf/cyber-security-senryaku-set.pdf>

(3)　「情報セキュリティ」と「サイバーセキュリティ」の包含関係については、「情報セキュリティ」が対象とする情報が紙などを含むことを根拠として「サイバーセキュリティ」よりも広範な概念を含むとする考え方もあり、定説があるわけではない。

表1　近年発生した主なサイバー攻撃事件

発生年	名称	概要
2010	Stuxnetによるイラン核施設へのサイバー攻撃	マルウェア（Stuxnet）を用いたイランの核施設を標的とした攻撃。施設の遠心分離機が稼働不能に陥ったとされる。
2011	ソニーPSNへの不正アクセス	ソニーが運営するコンピュータゲーム用サービス（PlayStation Network: PSN）が不正アクセスされ、利用者7700万人の個人情報が漏えいした。
2011	衆議院・参議院へのサイバー攻撃	衆参の議員等に対して添付ファイル付の標的型メールが送付され、添付ファイルを開いたPCが感染し、ID、パスワード等が漏えいした。
2012	Anonymousによるサイバー攻撃	オンライン上の匿名活動家集団であるAnonymousが、違法ダウンロード刑事罰化への抗議として、日本の政府機関のサイト等に対して攻撃を行った。
2012	JAXAに対するサイバー攻撃	宇宙航空研究開発機構（JAXA）の職員が利用していたPCがマルウェアに感染し、イプシロンロケットの仕様や運用に関する情報が漏えいした可能性がある。
2013	韓国の銀行や放送局へのサイバー攻撃	韓国の銀行や放送局を狙ったサイバー攻撃により、ATMやインターネットバンキングが停止する等の影響があった。
2013	外務省在外公館等に対するサイバー攻撃	外務省の在外公館の職員のPCが情報窃取を目的とした外務省向けに作成されたマルウェアに感染した。

（出典）各種資料を基に三菱総合研究所作成。

これらのサイバー攻撃は標的型攻撃と呼ばれる攻撃である。その多くはソフトウェアの脆弱性を利用したものであった。

2　安全保障とサイバーセキュリティ

近年、サイバー攻撃は安全保障上の主要課題として認識されてきている。表1に示したサイバー攻撃事件に見るように、国家安全保障に影響を与えかねないサイバー攻撃が多く発生している。これら攻撃事件が引き起こされた原因や状況などは必ずしも明確になっているわけではないが、例えば米国では、米企業に対するサイバー攻撃の容疑で中国軍関係者を訴追するなどの事例も発生している(4)。

これらを受けて、我が国においても2013年12月に国家安全保障会議決定・閣議決定された「国家安全保障戦略」の中で「国際公共財（グローバル・コモンズ）に関するリスク」として、サイバー空間の防護及びサイバー攻撃への対応能力を一層強化するよう明記している(5)。

2014年3月、防衛省ではサイバー攻撃の脅威に適切に対応するため、統合幕僚監部自衛隊指揮通信システム隊の下にサイバー防衛隊を新設した。サイバー防衛隊は、「防衛省・自衛隊のネットワークの監視及びサイバー攻撃発生時の対処を24時間体制で実施するとともに、サイバー攻撃に関する脅威情報の収集、分析、調査研究等を一元的に行います。」(6)とされている。

一方、安全保障の観点からは重要インフラ防護も重要である。我が国における重要インフラ

(4)　「米、中国軍関係者5人を訴追 サイバー攻撃の産業スパイ容疑で」『ロイター』2014.5.20. <http://jp.reuters.com/article/topNews/idJPKBN0DZ1A020140519>

(5)　「国家安全保障戦略について」（平成25年12月17日国家安全保障会議決定及び閣議決定）pp.7-8, 15. <http://www.cas.go.jp/jp/siryou/131217anzenhoshou/nss-j.pdf>

(6)　防衛省「サイバー防衛隊の新編について」2014.3.25. <http://www.mod.go.jp/j/press/news/2014/03/25d.html>

とは情報通信、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、クレジット、石油、化学の13分野である(7)。

重要インフラに対する主な攻撃事例を表2に示す。

表2　重要インフラに対する主なサイバー攻撃

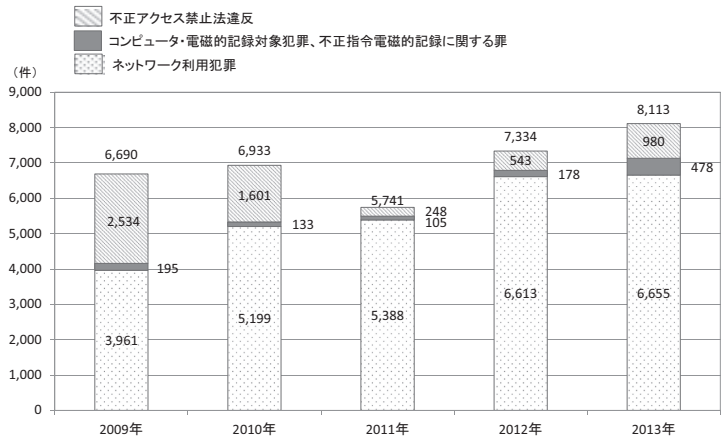
発生年	名称	概要
2000	上下水処理場への不正アクセス	豪Maroochy市の上下水処理場のシステムに元従業員が不正アクセスを行い、システムを誤動作させることで、汚水が公園や河川に流れ出した。
2003	原発監視制御システムのマルウェア感染	米Davis-Besse原子力発電所の監視制御システムにマルウェア（SQL Slammer）が感染、一部システムが数時間にわたって停止した。
2006	交通信号制御システムへの不正アクセス	米Los Angels市の交通監視センターの信号制御システムに対して元職員が不正アクセスを行い、交通信号を止めたことで、渋滞が発生した。
2008	クレジット決済会社への不正アクセス	英The Royal Bank of Scotland傘下のクレジット決済会社のコンピュータに東欧の犯罪者集団が不正アクセスしクレジットカードデータを窃取。日本を含む世界各国のATM2,100台から約8億円を盗んだ。
2010	Stuxnetによるイラン核施設へのサイバー攻撃	マルウェア（Stuxnet）を用いたイランの核施設を標的とした攻撃。施設の遠心分離機が稼働不能に陥ったとされる。
2013	韓国の銀行や放送局へのサイバー攻撃	韓国の銀行や放送局を狙ったサイバー攻撃により、ATMやインターネットバンキングが停止する等の影響があった。

（出典）各種資料を基に三菱総合研究所作成。

3　サイバー犯罪

インターネットが身近で不可欠なインフラとして利用されるようになるに伴い、インターネット等を利用したサイバー犯罪も増加している。図1に示すように、警察庁の発表によれば、2013年のサイバー犯罪の検挙件数は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」（児童買春・児童ポルノ法違反、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、出会い系サイト規制法違反、商標法違反）が6,655件（約82%）と大多数を占めている。

図1　サイバー犯罪検挙件数（日本）



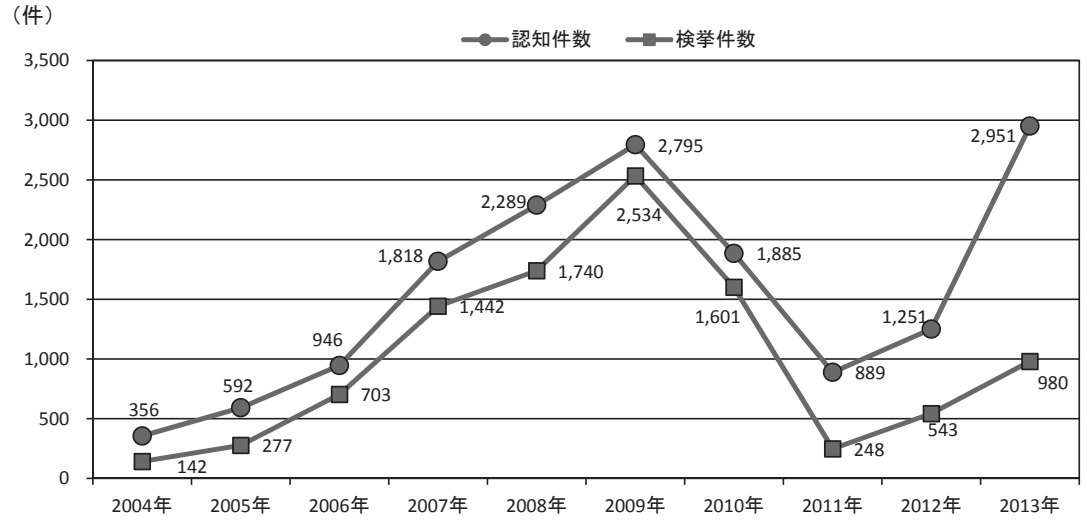
（出典）警察庁「平成25年中のサイバー犯罪の検挙状況等について」2014.3.27. <http://www.npa.go.jp/cyber/statics/h25/pdf01-2.pdf>を基に三菱総合研究所作成。

(7)　情報セキュリティ政策会議「重要インフラの情報セキュリティ対策に係る第3次行動計画」2014.5.19, p.8. <http://www.nisc.go.jp/active/infra/pdf/infra_rt3.pdf>

また、検挙件数全体に占める割合は低いものの、「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」は478件（前年比168.5%増）、「不正アクセス禁止法違反」は980件（前年比80.5%増）と、いずれも2012年と比べて急激に増加している(8)。

特に不正アクセスに関しては、警察庁の発表によれば、2013年の不正アクセス行為の「認知件数」は実に前年比1,700件増の2,951件であり、そのうち検挙された件数が980件、検挙率も33.2%（前年43.4%）と過去最低となっている（図2参照）。特に不正アクセス行為のうちインターネットバンキングの不正送金が1,325件と44.9%を占める(9)。

図2　不正アクセス行為の認知件数・検挙件数（日本）



（出典）警察庁「平成25年中の不正アクセス行為の発生状況等の公表について」2014.3.27. <http://www.npa.go.jp/cyber/statics/h25/pdf040.pdf>を基に三菱総合研究所作成。

インターネットバンキングに係る不正送金は、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。主な手口としては、被害者のPCにマルウェアを電子メールで送り込む手口や、ウェブサイトから巧妙にマルウェアをダウンロードさせる手口などが用いられている。マルウェアを介してインターネットバンキングのID、パスワード、乱数表等を窃取し、犯人の口座などに不正送金を行うものである。

そのほかのサイバー犯罪としては、秘密情報・個人情報の窃取や漏えいがある。近年は企業の秘密情報を持ち出して海外の競合他社に漏えいした事件や、個人情報を持ち出して名簿業者に販売するなどの事件が発生している。

国内で発生した最近の主なサイバー犯罪事件を表3に示す。

(8)　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. <http://www.npa.go.jp/cyber/statics/h25/pdf01-2.pdf>

(9)　警察庁「平成25年中の不正アクセス行為の発生状況等の公表について」2014.3.27. <http://www.npa.go.jp/cyber/statics/h25/pdf040.pdf>

表3　日本国内における最近の主なサイバー犯罪事件

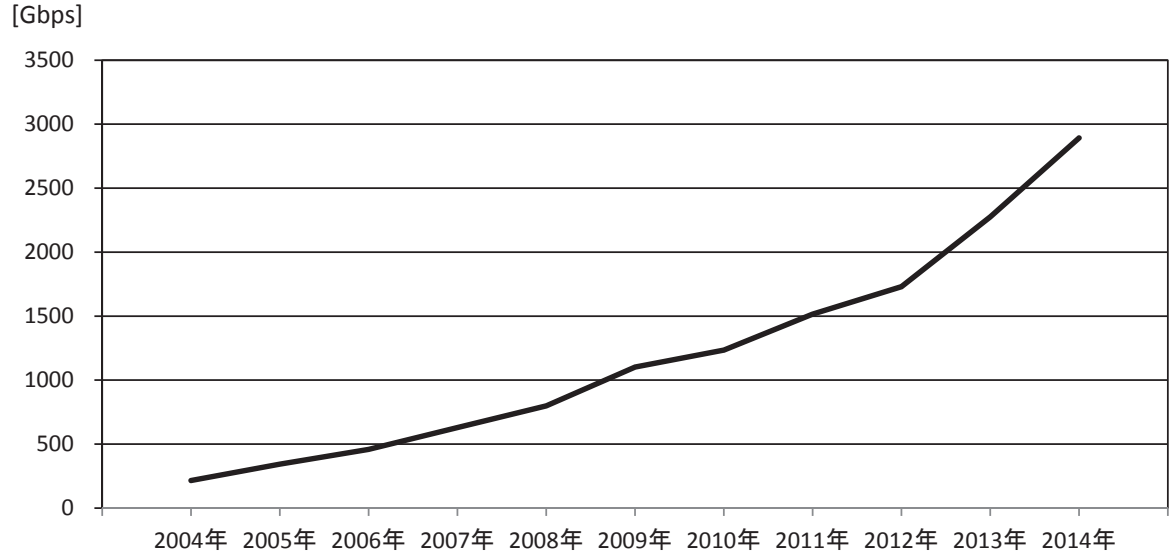
発生年	名称	概要
2012	パソコン遠隔操作事件	他人のPCを遠隔操作し、それを踏み台に小学校その他への襲撃や殺人等の犯罪予告を連続して行った事件で、IT関連会社社員を逮捕。
2013	フィッシングサイト開設事件	フィッシングサイトを開設した疑いで静岡県警が沖縄県の少年を逮捕。
2014	ベネッセ個人情報漏えい事件	ベネッセコーポレーションの顧客情報（約3504万件の個人情報）が、持ち出され、名簿業者に販売された事件で、同社のシステム開発・運用を行っているグループ会社の業務委託先の社員を逮捕。
2014	ネットバンキング不正送金事件	インターネットバンキングの不正送金事件で中国人13人を逮捕。不正送金で窃取した約6億円の大半を中国へ送金した。
2014	半導体技術の漏えい事件	東芝に勤務していた提携先社員が半導体の研究データを記録媒体にコピーして不正に持ち出し、韓国の半導体メーカーに漏えいした疑いで逮捕。

（注）上記には、現在も裁判継続中の事件が含まれている。
（出典）新聞報道等を基に三菱総合研究所作成。

4　情報通信技術の進展と社会的側面

情報通信技術、特にインターネットや携帯電話の普及は目覚しいものがある。例えば、米国の調査会社International Data Corporation（IDC）の推計によれば、2014年中に世界中で販売されたスマートフォンの販売台数は前年比26.3%増の約13億台に達する可能性があるとされる(10)。通信量（トラヒック量）で見た場合でも、その量は加速度的に増加している（図3参照）。図3は我が国のインターネット契約者が一秒間にインターネットからダウンロードしたデータ量を推計したものであり、2014年5月には前年同月比27.1%増の毎秒2.9テラビット（毎秒2,900ギガビット）に達したとされる。

図3　我が国のブロードバンド契約者の総ダウンロードトラヒック



（注）我が国のインターネット契約者が一秒間にインターネットからダウンロードしたデータ量を推計したもの。
（出典）総務省総合通信基盤局電気通信事業部データ通信課「我が国のインターネットにおけるトラヒック総量の把握」2014.10.7, p.2. <http://www.soumu.go.jp/main_content/000316564.pdf>を基に三菱総合研究所作成。

(10)“Worldwide Smartphone Growth Forecast to Slow from a Boil to a Simmer as Prices Drop and Markets Mature, According to IDC,”December 1, 2014. International Data Corporation Website <http://www.idc.com/getdoc.jsp?containerId=prUS25282214>

しかし一方で、情報通信技術の進展と普及は、狭義のセキュリティの枠には収まらない様々な問題を引き起こすようになっている。代表的な問題を以下に列挙する。

(1)　プライバシーの問題

スマートフォン、タブレット端末などが普及し、市民をとりまくネットワーク環境の利便性が高まり、一般化するとともに、そのような機器を利用する個人のデータ（パーソナルデータ）を利用したビジネスが活発化している。しかし、パーソナルデータについては、多くのデータを収集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、プライバシーに関する懸念が大きなものとなっている。

最近問題となった事例としては、東日本旅客鉄道（JR東日本）がSuica履歴情報の外部提供を行う事業を発表したところ、Suicaの利用者からの問合せやメディアからの批判が相次ぎ、提供を当面見合わせることとなった問題などがある(11)。

(2)　SNSの普及に伴う問題

利用者がインターネット等で交流するためのソーシャルネットワーキングサービス（Social Networking Service: SNS）を犯罪に悪用する者が現れるなど、様々な問題が発生している。例えば、SNSで「友人」や「同僚」として接近し、対象者の信頼を得た上で、機密情報を盗み出したり、マルウェアに感染させたりする標的型攻撃が既に海外で確認されている。国内でも何らかの方法で手に入れたIDとパスワード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、相手に購入させたプリペイドカードの情報を騙し取る詐欺事件が続発している(12)。また、SNSを介した出会い系サイトによって児童が被害を受けるケースや、SNSで特定の相手に執拗にメッセージを送り付けるサイバーストーカー行為も見られる。ほかにも、「ネットいじめ」や、他人を写した写真を勝手にSNS上に掲載することによるプライバシーや肖像権の侵害といった問題も発生している。

なかでも2013年以降、深刻な社会問題になっているのはSNSを通じた「炎上事件」(13)である。飲食店やコンビニエンスストア、交通機関などにおける不適切な行為の写真を投稿したことにより、その不適切な行為を行った本人が非難されるだけでなく、行為が行われた店舗や企業の管理責任が問われ、その中には閉店に追い込まれたケースもあるなど、企業にとっての新たなリスクとなっている(14)。さらに、不適切な行為を行った人物に関する個人情報を調べ上げて公開するなど、執拗にバッシングするネット上の私刑も問題視されている。

(3)　子どものサイバー犯罪被害

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。子どもたちにも急速に普及しているSNSなどを使った、特定の児童生徒に対する誹謗・中傷を行う「ネットいじめ」

(11)　東日本旅客鉄道「Suica に関するデータの社外への提供における対応について」2013.9.20. <http://www.jreast.co.jp/press/2013/20130913.pdf>
(12)「LINE乗っ取り、被害総額2800万円　警視庁、電子マネーなど詐取」『朝日新聞』2014.10.29, 夕刊.
(13)「炎上事件」とは不祥事などを契機として、インターネット上のサイトやコメント欄などに大量に非難や中傷のコメントが書き込まれる事件をいう。サイバーカスケードとも呼ばれる。
(14)　ローソン「加盟店従業員の不適切な行為についてのお詫びとお知らせ」2013.7.15. <http://www.lawson.co.jp/emergency/detail/detail_78348.html>

や、出会い系サイトやコミュニティサイトを利用した児童買春等の被害にあうケースは深刻な社会問題となっている。また、不用意にアクセスしたサイトから不当に高額な請求を受ける被害も発生している。

(4)　ネット依存・スマホ依存

インターネットやスマートフォンの利用時間をコントロールできず、これらがないと苛立ちや不安感等を覚えるなど、生活への支障をきたす、いわゆるネット依存、スマホ依存の問題が広がっている。ネット依存、スマホ依存は、十分な情報リテラシーを習得していない青少年に多く見られる傾向がある。

ネット依存、スマホ依存の影響としては、引きこもり気味になる、健康状態が悪化する、遅刻・欠席しがちになるなどの問題に加え、児童・生徒の場合は学力への悪影響も懸念されている(15)。

近年では、スマートフォンの普及に伴い、SNSへの依存傾向も強くなっている。SNSの場合、友達間で際限なく続くコミュニケーションに区切りを付けるのが難しく、また実世界の人間関係の悪化や仲間はずれなどをおそれてSNSに没頭してしまう面がある。

(5)　電子商取引に係るトラブル

電子商取引に係る代表的なトラブルとしてはインターネットショッピングやインターネットオークションに係る詐欺がある。詐欺は犯罪行為として取締りの対象となっているが、電子商取引の場合、取引相手の顔が見えないなどの特徴があるためトラブルになりやすい。

それ以外のトラブルとしては、契約成立時点が分かりにくいなどの電子商取引に固有の問題がある。経済産業省では、民法を始めとする関係法律がどのように適用されるのかを明らかにし、取引当事者の予見可能性を高め、取引の円滑化に資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(16)。

また、「無料」といった表示、全体として消費者に誤解を与え得るような表示や、ステルスマーケティング(17)として、口コミサイト(18)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、一般消費者の誤認を誘うことが問題となっている。さらに電子商取引がグローバル化する中で、国境をまたぐ越境電子商取引による問題も発生している。

(6)　電子マネーのリスク

プリペイド型の電子マネーの利用が進んでいるが、店舗の店員等が不正な処理等を行うことで不正なチャージを行うケースが発生している。またSNS等のアカウントを乗っ取り、本人になりすまし、その知人をだまして電子マネーをチャージさせる詐欺事件も発生している。

---

(15)「ネット依存で成績低下　1日4時間超　正答率最低　学テ小中生分析」『東京新聞』2013.12.26.
(16) 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>
(17) ステルスマーケティングとは、ある特定の商品の宣伝であることを消費者に隠して行う宣伝や広報活動のこと。
(18) 口コミサイトとは商品やサービス、企業などに対する個人の意見が書き込まれたサイトのこと。

III　情報セキュリティの歴史

サイバーセキュリティについて体系的な理解を行うためには、その歴史的な背景について理解することが必要である。本章ではサイバーセキュリティの前史として、情報通信技術が登場する以前から存在していた情報セキュリティの歴史について概観する。

1　第二次世界大戦以前

情報セキュリティの考え方は情報通信技術の進展する遥か前から人類の歴史に登場してきている。情報セキュリティの重要な要素技術である暗号は、紀元前から利用されていることが知られている。一例としては、紀元前5世紀のギリシャで利用されたスパルタの暗号（棒と革紐を用いた暗号）、紀元前1世紀のローマでユリウス・カエサルが用いたとされるシーザー暗号などがある。このように、暗号技術は軍事技術の一つとして数千年にわたり利用され、発展してきた。

その後、無線技術とモールス信号の登場、コンピュータの登場（米ENIAC、1946年開発）、マイクロプロセッサ「Intel 4004」の開発（1971年発売）、インターネットの発明（ARPANET、1965年開発開始）等があり、新しい技術の登場はそれに対する攻撃技術の開発を促した。この流れがサイバーセキュリティとつながっている。

情報セキュリティのもう一つの流れとしては情報保証（Information Assurance）がある。情報保証とは簡単にいえば、情報セキュリティ（機密性・完全性・可用性等）を維持することと、そのための組織的な取組を指す。情報を重要性で分類し、重要度に応じて管理を行うという情報保証の基本となる考えは、第二次世界大戦前から存在している。本格的に情報保証が体系化されたのは、19世紀に入ってからで、例えば英国の1889年公務秘密法（Official Secrets Act 1889）等にその例を見ることができる。第一次世界大戦頃には、複数階層からなる情報分類方法（例：「機密」、「極秘」、「秘」等）が英国などで確立した。

2　第二次世界大戦と情報セキュリティ

第二次世界大戦期には、情報通信技術が大きく発達し、後のサイバーセキュリティにつながる要素技術が登場した。特に19世紀末に開発された無線通信技術が広く普及し、外交・軍事用に無線通信が活用されるようになると、暗号の利用が不可欠となり暗号技術の重要性が高まった。これは、無線通信技術が本来的に持つ誰でも受信可能という性質のためである。

1918年、ドイツのアーサー・シュールビウス（Arthur Scherbius）により発明され、1925年にドイツ軍に採用された電気機械式暗号装置エニグマによって、従来ほとんど手作業により行われていた暗号化・復号の作業の自動化が可能となった。

一方で、暗号文から平文（元の文書）を求める暗号解読についても、これまで以上の労力が割かれるようになり、大量の人員が投入されるとともに、新しい暗号解読装置の開発が進められた。この暗号解読装置の開発は後のコンピュータの開発につながる。

英国では暗号解読のため、政府暗号学校（Government Code and Cypher School: GC&CS,通称：ブレッチリーパーク（Bletchley Park））を設置し、第二次世界大戦期には人員1万人を数えた。GC&CSは

数学者を雇用した。エニグマの暗号文は数学者のアラン・チューリング（Alan Mathison Turing）らにより専用解読機械を用いて解読された。またGC&CSでは暗号解読のため、Colossusと呼ばれるプログラム可能な電子計算装置の一種を開発した。Colossusはコンピュータの実用化に向けた黎明期の成果の一つである。GC&CSは1946年に政府通信本部（Government Communications Headquarters: GCHQ）に改編され、現在でも英国の暗号解読業務等を担当している。(19)

第二次世界大戦中、米国では暗号解読のためSSA（Signal Security Agency）が設置され、日本の外交用暗号、海軍用暗号を解読した。SSAは英国のGC&CSとも協力を行い、ミッドウェー海戦の米側勝利や山本五十六連合艦隊司令長官搭乗機の撃墜などの戦果につなげている。SSAは第二次世界大戦後、軍保安局を経て1952年に国家安全保障局（National Security Agency: NSA）に改編され、現在でも米国の諜報機関として通信傍受等の活動を行っている。(20)

日本軍も米英仏中の外交暗号と中ソの軍事暗号の一部を解読していたとされる。敗戦時に暗号解読に関する資料等は真っ先に破棄されたため、詳しい情報は残っていないが、暗号解読は十分に外交政策や作戦に活用されていなかった。(21)

第二次世界大戦が情報通信技術の発展に大きな影響を与えた最大のものが、コンピュータの発明である。一般には、1946年に米国陸軍の弾道計算用に開発されたENIACが有名であるが、前に示したColossusもコンピュータの先駆的な業績として知られている。

Ⅳ　サイバーセキュリティの歴史

前章ではコンピュータ登場前までの情報セキュリティの歴史を示したが、本章では第二次世界大戦期間中に開発されたコンピュータをはじめとする情報通信技術の進展と、サイバーセキュリティの歴史について概観する。

1　コンピュータの商用利用の進展【第二次世界大戦後～1995年頃】

コンピュータは第二次世界大戦後しばらくは専ら軍事用の装置であったが、政府機関、大学等の研究機関や民間企業で利用されるようになってきた。また、インターネットも当初軍事用の通信ネットワークとして開発されたが、大学等の研究機関を中心に普及が進んできた。さらに、1995年にWindows 95が発売されたことをきっかけに、PCとインターネットは一般に普及することになった。本節では1995年頃までの情報通信技術の発展とサイバーセキュリティについて述べる。

（1）　1950年代から1960年代

1950年代は、1951年にサンフランシスコ講和条約が結ばれ日本が国際社会に復帰する一方、1950年には朝鮮戦争が勃発するなど、米ソの対立が深まった時代である。

第二次世界大戦後、コンピュータと通信技術は軍事用から民生用途に広がっていった。1951

(19)　Intelligence Services Act 1994に、GCHQの業務として、“to obtain and provide information derived from …（中略）…encrypted material”が規定されている。
(20)　“Mission.”National Security Agency Website <https://www.nsa.gov/about/mission/index.shtml>
(21)　小谷賢「日本軍とインテリジェンス―成功と失敗の事例から―」『防衛研究所紀要』11巻1号, 2008.11, pp.43-68. <http://www.nids.go.jp/publication/kiyo/pdf/bulletin_j11_1_3.pdf>

年には世界初の商用コンピュータであるUNIVAC-I（ユニバックワン）が発売された。1952年にはIBMから初の商用メインフレームコンピュータ(22)とされるIBM701が、1953年には世界初の大量生産されたコンピュータとされるIBM650が発表された。UNIVAC-I 、IBM701、IBM650はいずれも真空管を用いたコンピュータであった。

東京証券取引所と野村證券が1955年に導入したUNIVAC-120が日本初の商用コンピュータといわれている(23)。その後1959年には三和銀行（現：三菱東京UFJ銀行）がIBM650を導入した。これが日本の銀行として初めてのコンピュータ導入である。

1960年代は、高度成長期として日本経済が大きく発展した時代である。1964年には東海道新幹線が開通し、東京オリンピックが開催された。一方で、ベトナム戦争の勃発をはじめとして東西冷戦が激化した。冷戦下の米ソ宇宙開発競争により1969年にアポロ11号が月着陸に成功したが、米ソの軍事技術・宇宙技術の開発競争はコンピュータの性能向上にも大きく寄与した。1964年にIBMが開発したメインフレームコンピュータSystem/360では、現在のコンピュータにつながる様々な概念・技術が実用化されている。具体的にはオペレーティングシステム、バーチャルマシン（仮想機械）等であり、System/360のコンピュータアーキテクチャ（基本設計）は現在のコンピュータの基礎となっている。

我が国では1960年には日本国有鉄道（現：東日本旅客鉄道ほか）が大規模オンライン座席予約システムを稼働させるとともに、三井銀行（現：三井住友銀行）が1965年に日本初の銀行オンラインシステムを構築するなど、オンラインシステムが社会に広まってきた。

1960年代半ば以降になると、一般企業におけるコンピュータ利用も活発化してくる。米国の先進的な企業におけるコンピュータ利用の考え方である経営情報システム（Management Information System: MIS）が我が国に紹介されたのも1960年代半ばである。1965年に設立された日本電子計算開発協会（現：日本情報経済社会推進協会（JIPDEC））(24)は、日本生産性本部との共催で米国のMIS動向を調査するための使節団を組織し、その報告書(25)は我が国企業におけるコンピュータ導入を促進したとされている。

コンピュータやオンラインシステムの発達と並行して、現在のインターネットやWebにつながる技術の萌芽がこの頃に開発されている。具体的には以下のような技術である。

- 米国国防総省による後のインターネットとなるARPANET（アーパネット）の開発開始（1965年）
- テッド・ネルソン（Theodor Nelson）による後のWebにつながる、複数のテキストを相互に関連付ける仕組みであるハイパーテキスト（Hypertext）の概念提唱（1965年）
- AT&Tベル研究所によるオペレーティングシステムUNIXの研究開始（1969年）

(22) メインフレームコンピュータとは、基幹業務用に用いられる大型コンピュータのことで、汎用コンピュータ等と呼ばれることがある。
(23)「日本ユニシスグループの歴史」日本ユニシスウェブサイト <http://www.unisys.co.jp/com/history.html>
(24) 日本情報経済社会推進協会（JIPDEC）は、日本電子工業振興協会の電子計算機センターを継承して1967年に設立された日本情報処理開発センター（JIPDEC）、1968年に設立された日本経営情報開発協会（CUDI、1973年に日本情報開発協会に改称。）、1970年に設立された情報処理研修センター（IIT）の3団体が1976年に統合して発足したものである。発足当時は日本情報処理開発協会（JIPDEC）であったが、2011年に日本情報経済社会推進協会（JIPDEC）に改称された。
(25) 日本生産性本部ほか編『アメリカのMIS―訪米MIS使節団報告書―』ぺりかん社, 1968.

（2）　1970年代から1980年代

1970年代はオイルショックが発生し、我が国の経済も高度経済成長期から安定成長期に移行した。

情報通信技術の分野では、1971年当時に世界最初のマイクロコンピュータ（マイコン）であったIntel 4004が米国Intel社から発表され、1977年には個人向けの完成品PCとして最初期の一つであるApple IIが米国Apple社から発売された。

暗号技術の分野では、1976年に公開鍵暗号に関する世界最初の論文が公表され、翌1977年には現在でも広く使われている公開暗号方式であるRSAが発表された。1977年には、共通鍵暗号方式の領域でもその後30年間にわたって広く使われることになる標準暗号DES（Data Encryption Standard）が米国国立標準局（National Bureau of Standards: NBS, 現：米国国立標準技術研究所（National Institute of Standards and Technology: NIST））により選定されている。

我が国におけるコンピュータの普及は主に企業において進んだ。1970年代になると意思決定支援システム（Decision Support System: DSS）が注目を浴びた。情報処理振興事業協会（現：情報処理推進機構（IPA））が設立されたのもこの頃（1970年）である。1970年代後半からは、オフコン・ワープロ・表計算ソフトなどからなるオフィスオートメーション（OA）の導入が急速に進んだ。

企業における情報システムの導入が進む中で、情報システムの信頼性確保が重要となってきたことから、システム監査の考え方が1960年代後半から1970年代にかけて普及してきた。1966年には日本電子計算開発協会が国税庁に対して「電子計算機利用度向上に伴う税務調査関係証憑取扱いに関する要望書」を提出している。これは会計帳簿としてコンピュータの磁気記録媒体による保存を認めるように求めたものであるが、これは一方で、企業にとっても会計システムの信頼性を示す必要が出てきたことを意味している。1969年には日本経営情報開発協会（現：JIPDEC）が、学識経験者、経済団体連合会、日本公認会計士協会、大蔵省（現：財務省）、国税庁、通商産業省（現：経済産業省）、法務省などからなる「会計税務研究委員会」を組織し、企業会計にコンピュータを活用する際の課題等について検討を行った。1975年には日本情報開発協会（現：JIPDEC）がシステム監査委員会を設置し、検討の結果を1980年に「システム監査基準（試案）」等として公表し、1985年に通商産業省は「システム監査基準」を策定した。

1980年代は、米国のレーガン大統領や英国のサッチャー首相などによる新保守主義的な政策が進められたことで、東西両陣営の軍拡が行われたが、ソ連の財政破綻等を早める結果につながり、1989年の米ソ首脳のマルタ会談により冷戦が終結した。

情報通信技術の分野では1980年代にPCの普及が本格化した。PC用のオペレーティングシステムであるMicrosoft MS-DOSが1981年にIBM PC用にリリースされ(26)、1982年にはIBM以外にも供給開始された。日本でもNEC PC-9801が1982年に発売され、企業を中心に広く普及した(27)。また、インターネットが本格的に普及を始めたのは1980年代である。1982年には米国国防総省がインターネットの中核技術であるTCP/IPを標準通信プロトコルに決定し(28)、1984年に日本にもインターネットが導入された（慶應義塾大学と東京工業大学がJUNETにより接続）。イ

(26)　当時はPC-DOSと呼んだ。
(27)「コンピュータ博物館」情報処理学会ウェブサイト <http://museum.ipsj.or.jp/computer/personal/0011.html>
(28)　現在はインターネット技術タスクフォース（Internet Engineering Task Force: IETF）でTCP/IPに関する提案や標準化作業が行われている。

ンターネットではないが、1985年に日本初の商用パソコン通信サービスであるアスキーネットが開始されている。また、家庭用の情報機器の普及も1980年代に進んだ。1982年にはコンパクトディスク（CD）プレーヤーが、翌1983年には家庭用ゲーム機である任天堂ファミリーコンピュータが発売された。

サイバーセキュリティの分野では、1980年代に初のコンピュータウイルスが作成されている。その起源には諸説あるが、Apple IIに感染するElk Clonerウイルス（1982年）、IBM PCに感染する初のウイルスBrain（1986年）等が初期のウイルスとして記録されている。1988年にはインターネットを介して感染拡大する初のウイルスであるMorrisワームが作成され、数千台のコンピュータに感染した。この事件を契機に世界初のコンピュータセキュリティインシデント対応チーム（Computer Security Incident Response Team: CSIRT）としてComputer Emergency Response Team/ Coordination Center（CERT/CC）が1988年に米国で設立された。

一方、我が国でも1970年代に始まった情報システムの信頼性を確保する取組はさらに広がり、金融分野でも、1984年に金融情報システムセンター（The Center for Financial Industry Information Systems: FISC）が設立された。FISCは1985年に「金融機関等コンピュータシステムの安全対策基準」、1987年に「金融機関等のシステム監査指針」を策定している。

コンピュータ利用犯罪もこの頃から発生している。1970年には最初期のコンピュータ利用犯罪として日経マグロウヒル社（現：日経BP社）の購読者名簿が盗難・複製され、リーダーズ・ダイジェスト社の広告発送に使われる事件が発生している(29)。1981年に銀行員がオンラインシステムを不正操作し1億8000万円を横領したいわゆる三和銀行オンライン詐欺事件が発生したが、それ以外にもキャッシュカード偽造事件である近畿相互銀行オンライン事件も1981年に発生している。これらの事件を契機として、1987年に「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」等が刑法に新設された。

1980年代になると個人情報の保護についても関心が高まった。経済協力開発機構（Organisation for Economic Co-operation and Development: OECD）理事会が1980年に公表した「プライバシー保護と個人データの国際流通についてのガイドライン」（いわゆる「OECDプライバシーガイドライン」）は、その後のEUの「個人データ取扱いに係る個人の保護及び当該データの自由な移動に関する1995年10月24日の欧州議会及び理事会の95/46/EC指令」（いわゆる「EUデータ保護指令」）や日本の「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）の制定につながることになる。

（3）　1990年代前半

1990年代前半は、1991年のソ連邦崩壊による東西冷戦終結など、政治体制の面で大きな変動があった。情報通信技術の分野では、1990年に欧州原子核研究機構（European Organization for Nuclear Research: CERN）のティム・バーナーズ＝リー（Tim Berners-Lee）がWWW（World Wide Web）サーバとブラウザを開発・実装、1993年にはイリノイ大学の米国立スーパーコンピュータ応用研究所（National Center for Supercomputing Applications: NCSA）のマーク・アンドリーセン（Marc Lowell Andreessen）らが画像も扱えるMosaicブラウザを開発し公開したことで、WWWの普及は急速に進んだ。1994年にはYahoo!がウェブサイトを開設している。

(29)「磁気テープから情報盗む　購読者名簿つつ抜け　電算機で翻訳中複写」『朝日新聞』1971.2.3.

1993年には郵政省（現：総務省）がインターネットの商用利用を許可したことで、同年、日本初のインターネットサービスプロバイダ（Internet Service Provider: ISP）としてインターネットイニシアティブがサービスを開始した。

また、1991年にはフィンランドのヘルシンキ大学院生であったリーナス・トーバルズ（Linus Torvalds）がLinuxオペレーティングシステムを開発した。なお、LinuxはUNIX互換のオペレーティングシステム環境であるGNU（グニュー）等とともにオープンソースソフトウェアが広まるきっかけとなった。

東西冷戦の終結は、米国の暗号政策に大きな影響を与えることになった。従来の暗号技術は軍事技術として政府が厳格に管理し、一般には限定的に利用が認められるにとどまっていたが、暗号技術の民間開放を訴える活動であるサイファーパンク（Cypherpunk）が米国を中心に広がりを見せた。1992年にはサイファーパンク活動を推進するためのメーリングリストが開設され、1994年には暗号輸出規制に反対するため暗号ソフトのソースコードが印刷され出版された(30)。さらに米国の暗号学者ダニエル・バーンスタイン（Daniel Bernstein）は米国のNPOである電子フロンティア財団（Electronic Frontier Foundation: EFF）の支援を受け、暗号ソフトのソースコードの公開を禁止するのは言論の自由に関する憲法違反であるとして政府に対する訴訟を起こした。この裁判の結果、1996年に連邦裁判所においてバーンスタインの訴えが認められたことを契機として、1996年には暗号輸出規制が緩和されるなど米国の暗号政策は大きく自由化の方向に転換していった。この暗号規制の緩和は、インターネットや電子商取引の安全性の向上につながりその普及を支えた。

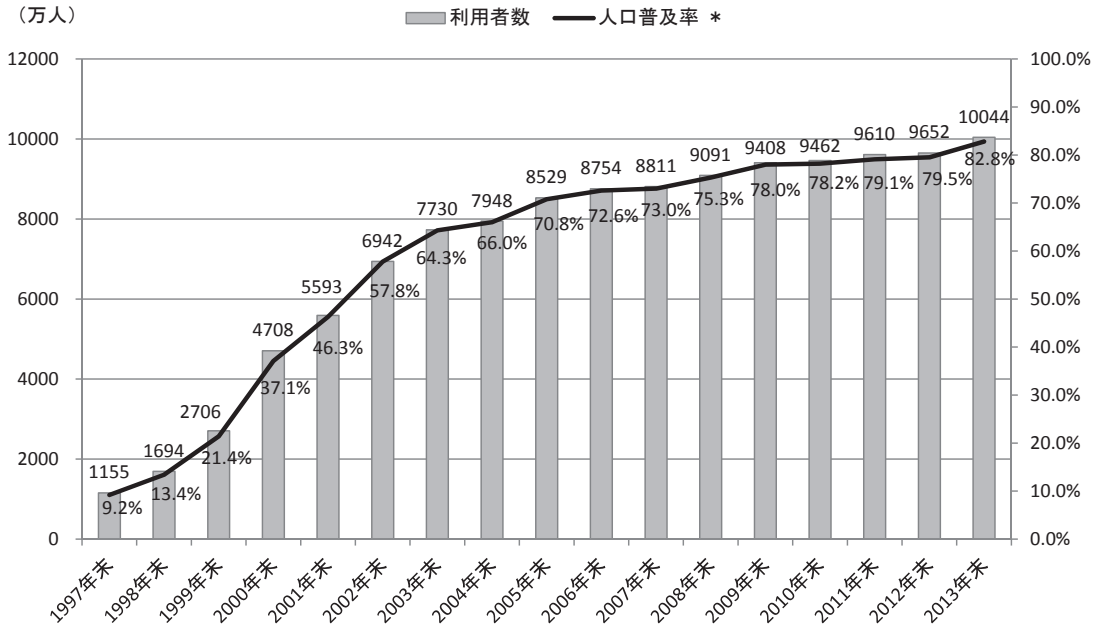
2　インターネットの一般への普及とニューエコノミー【1995年～2000年前後】

米国では1995年から2000年前後は、IT投資の活発化やIT企業の台頭によりニューエコノミーと呼ばれる好景気が続いた。一方で、日本ではバブル経済の崩壊に続く「失われた10年」の中で、景気低迷が続いていた。1995年には阪神・淡路大震災、地下鉄サリン事件等が発生した。

情報通信技術の分野では、1994年のNetscapeブラウザの公開、1995年のWindows 95の発売などを契機として、日本でも一般利用者に急速にインターネットが普及していった（図4参照）。1997年前後には日本のインターネット利用者数が1000万人を突破した。

(30)　書籍の輸出は認められていた。

図4　インターネット利用者数及び人口普及率の推移（日本）



（＊）人口普及率とは、インターネット利用者数を国勢調査及び生命表を用いて推計した各年の6歳以上人口で除したものである。

（出典）総務省「平成20年「通信利用動向調査」の結果」2009.4.7. <http://www.soumu.go.jp/johotsusintokei/statistics/data/090407_1.pdf>; 総務省「平成25年通信利用動向調査の結果」2014.6.27. <http://www.soumu.go.jp/johotsusintokei/statistics/data/140627_1.pdf>を基に三菱総合研究所作成。

1995年には米国でAmazon.comサービスが開始され、翌1996年には日本で電子商取引推進協議会（ECOM）が発足するなど、電子商取引も活発化した。1997年には住友銀行（現：三井住友銀行）が国内初のインターネットバンキングサービスを開始した。そのほか、無線LAN規格であるIEEE 802.11が1998年に発行され、1999年にNTTドコモのiモードサービスが開始されるなど、モバイル系の技術・サービスが登場した。

サイバーセキュリティ分野では、1995年に米国で「最強のハッカー」と称されたケビン・ミトニック（Kevin Mitnick）が逮捕されたが、その後も大規模な不正アクセス事件が続いた。1999年には米国ホワイトハウス、連邦議会上院、連邦捜査局（Federal Bureau of Investigation: FBI）のサイトが相次いでDoS（Denial of Service）攻撃を受け一時サービス停止に追い込まれる事件が発生した。

個人情報関連では、1999年に京都府宇治市で約21万人の住民基本台帳データが漏えいする、自治体による初めての大規模な個人情報流出事件が発生している。また、欧州では1995年にEUのデータ保護指令が制定されるなど、個人情報保護に対する機運が高まっていた。日本でも1999年にJIS Q 15001:1999「個人情報保護に関するコンプライアンス・プログラムの要求事項」が制定され、同年、日本情報処理開発協会（現:日本情報経済社会推進協会）はプライバシーマーク制度の運用を開始している。

電気や水道などの人々の生活を支える重要インフラにも情報システムやインターネットが利用されるようになると、ネットワークを介した重要インフラへのサイバー攻撃などの新しい脅威が問題になってくる。インターネットの普及が進んでいた米国では、テロ攻撃などへの懸念もあり、「重要インフラ防護についての大統領指令」（Presidential Decision Directive No. 63: PDD63）が1998年に発布された。

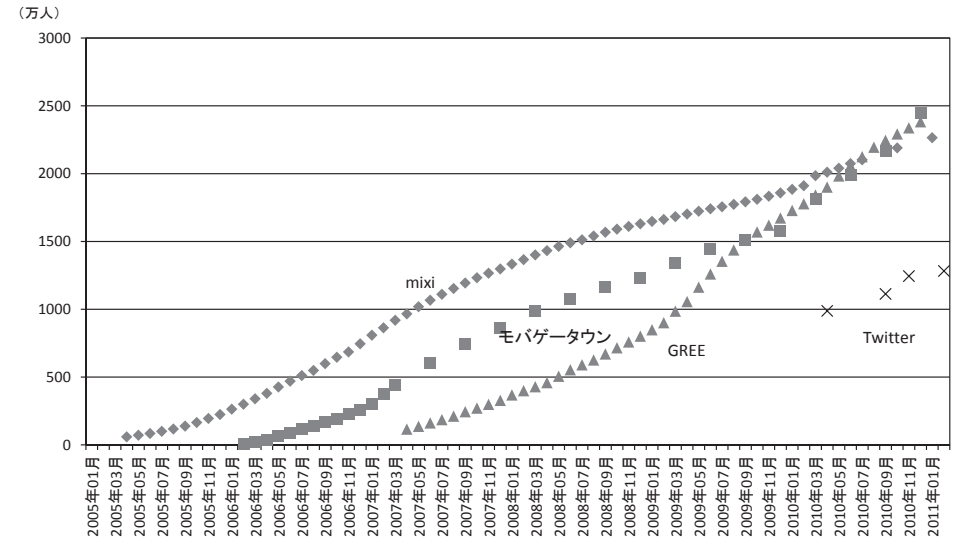
3　米国同時多発テロの発生とインターネットバブルの崩壊【2000年～2005年前後】

2000年前後、米国のインターネットバブルが頂点に達した。1999年にはAmazon.comの創業者ジェフ・ベゾス（Jeffrey Bezos）がタイム誌の「今年の人」に選定された。2000年1月3日には、Yahoo!の株価が最高で475ドルにまで達するなど、IT企業に対する評価が過大になっていた。2001年頃になると、一転してインターネットバブルが崩壊する。また2001年には同時多発テロが発生して、米国は景気後退の中でテロとの戦いに巻き込まれていった。

同時多発テロを契機に2001年に、米国では大統領令13231（Executive Order13231: E.O.13231）を発行しサイバーテロ対策の強化が進められるとともに、重要インフラ防護体制も再整備され、PDD63は「国土安全保障に関する大統領指令第7号」(Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection: HSPD-7）として改訂された。HSPD-7により国土安全保障省（Department of Homeland Security: DHS）が重要インフラ防護の主導機関となり、DHSを中心とした重要インフラ防護の実行戦略として、2006年に「国家インフラ防護計画」（National Infrastructure Protection Plan: NIPP, 2013年最終改訂）が策定された。また政府機関の情報セキュリティ対策の向上にも力を注ぎ、2002年には「連邦情報セキュリティ管理法」（Federal Information Security Management Act of 2002: FISMA, Title III of the E-Government Act of 2002, P.L. 101-576）が成立した。

情報通信技術の分野では、SNSの普及が本格的に始まったのが2005年前後である（図5参照）。mixi（2004年、日本）、Facebook（2004年、米国）、YouTube（2005年、米国）、Twitter（2006年、米国）等、主要なサービスがこの時期に開始されている。なお、LINEのサービス開始（日本）は少し遅れて2011年である。

図5　日本における主要なSNSサービスの利用者数の推移



（出典）総務省通信国際戦略局情報通信経済室「ICT インフラの進展が国民のライフスタイルや社会環境等に及ぼした影響と相互関係に関する調査研究報告書」2011.3, p.50. <http://www.soumu.go.jp/johotsusintokei/linkdata/h23_06_houkoku.pdf>を基に三菱総合研究所作成。

また、2000年前後にはファイルやデータの交換を分散したPCで実現する技術であるP2P（Peer To Peer,「ピアトゥピア、ピーツーピー」と読む。）技術が実用化された。1999年に米国で音楽ファ

イル共有システムNapsterがサービスを開始したのに引き続き、日本でも2002年にファイル共有システムWinnyが公開された。P2P技術は有力な技術であったが、一方で音楽ファイルや動画、漫画などのコンテンツを不正に共有するために用いられることも多く、著作権法の観点から問題になった。2004年にはWinny開発者の金子勇東京大学特任助手（当時）が著作権侵害行為幇助の罪で逮捕された（2011年に最高裁にて無罪確定）。P2P技術開発者の逮捕は、P2P技術を開発する研究者を萎縮させ、技術開発の停滞を招いたとの批判もある(31)。

サイバーセキュリティ分野では、Code Red（2001年）、Nimda（2001年）、SQL Slammer（2003年）等のウイルスが大流行し、世界的なネットワーク障害が発生するなど深刻な被害が発生した。2000年にはYahoo!、Amazon、eBay、CNN等に対する大規模なDDoS（Distributed Denial of Service）攻撃も発生している。我が国でも2000年に中央省庁Web改ざん事件が発生した。これは中国語を使うハッカー集団による攻撃といわれており、科学技術庁、総務庁、運輸省（いずれも当時）、参議院等のウェブサイトが中国語等のページに改ざんされた(32)。この事件の影響もあり、2000年に日本政府は内閣官房に「情報セキュリティ対策推進室」を設置し、省庁横断的な情報セキュリティ対策の強化が図られた。情報セキュリティ対策推進室は2005年に「内閣官房情報セキュリティセンター」（現：内閣サイバーセキュリティセンター（NISC））に改組されるとともに、内閣官房長官を議長とする「情報セキュリティ政策会議」が設置された。以降、多少の変更はあるものの、情報セキュリティ政策会議を「わが国の情報セキュリティ戦略に関する問題の根幹に関する事項を決定する母体」とし、NISCが関連省庁と連携しながらサイバーセキュリティ問題に対する取組を進めていくこととなった（概論「サイバーセキュリティに関する法律及び制度」図1参照）(33)。

サイバー犯罪については、警察庁が2001年に「サイバーテロ対策技術室」（サイバーフォースセンター）を設立するなど、対応体制の構築が進められた。サイバー犯罪は国境をまたぐ犯罪が多いことから、2001年には「サイバー犯罪に関する条約（Convention on Cybercrime）」（いわゆる「サイバー犯罪条約」）が採択された。国内では、2004年に同条約の締結が衆参両院で承認され、2012年に公布及び告示（平成24年条約第7号）、同年11月に効力が発生した。国際的なサイバーセキュリティ確保に向けた取組の一環として、OECDは2002年に「OECD 情報システム及びネットワークのセキュリティのためのガイドライン：セキュリティ文化の普及に向けて」（OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security）を公表した(34)。同ガイドラインでは、ネットワークへの全ての参加者が情報システムとネットワークを守るために適切な行動を取る責任について認識することを「セキュリティ文化」として広めていくよう求めている。またこれらの行動は、オープンで自由な情報の流通、プライバシーへの配慮な

(31)「Winny事件はソフト開発者を萎縮させる？」『ITmediaニュース』2004.6.28. <http://www.itmedia.co.jp/news/articles/0406/28/news066.html>

(32) 情報処理振興事業協会セキュリティセンター『情報セキュリティの現状 2000年版』2001, p.165. <http://www.ipa.go.jp/security/fy12/sec2000/sec2000.pdf>

(33) 内閣官房情報セキュリティセンター「情報セキュリティ政策会議の設置について」2005.5.30. <http://www.nisc.go.jp/conference/seisaku/pdf/050530seisaku-press.pdf>　なお、2015年1月9日のサイバーセキュリティ基本法の全面的施行にともない、内閣官房情報セキュリティセンターは「内閣サイバーセキュリティセンター」に改組された。情報セキュリティ政策会議の決定事項及び検討事項等についてはサイバーセキュリティ戦略本部に引き継がれた。

(34) Organisation for Economic Co-operation and Development, "OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security," 2002. <http://www.oecd.org/internet/ieconomy/15582260.pdf>

ど、民主主義の原則と整合が取れている必要がある点についても明示している。

2004年に発生したYahoo! BB顧客情報漏えい事件では、450万人分もの顧客情報が漏えいするなど、これまでとは比較にならない規模の情報漏えい事件が発生し、これを契機に、企業においても個人情報保護やサイバーセキュリティの確保が重要な経営課題となってきた。2000年には組織における情報セキュリティを管理するための仕組みとして情報セキュリティマネジメントシステム（Information Security Management System: ISMS）に関する初の国際標準としてISO/IEC 17799:2000（後のISO/IEC 27002）が策定され、これらに基づきJIPDECが2002年にISMS評価制度の運用を開始した。また2003年には情報セキュリティマネジメントが適切になされているかを監査するための制度として、経済産業省による情報セキュリティ監査制度が開始されるとともに日本セキュリティ監査協会（JASA）が設立されている。2005年には個人情報保護法が施行された。

また、2002年に発生した重症急性呼吸器症候群（Severe Acute Respiratory Syndrome: SARS）の経験から、災害時等における組織の事業継続管理の重要性が認識され、事業継続計画（Business Continuity Plan: BCP）の策定が求められるようになってきた。情報通信についても、その停止が組織の事業継続に大きな影響を与えることから、情報通信障害発生時の計画（IT-BCP）の策定が求められるようになっている(35)。

また、2001年頃には迷惑メール（スパムメール）、フィッシングメールや出会い系サイトなどが社会問題化した。迷惑メールの送信を規制するために「特定電子メールの送信の適正化等に関する法律」（いわゆる「特定電子メール法」。平成14年法律第26号）、「特定商取引に関する法律の一部を改正する法律」（平成14年法律第28号）が、出会い系サイトを規制するために2003年に「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」（いわゆる「出会い系サイト規制法」。平成15年法律第83号）が制定された。

4　スマートデバイス・クラウドの普及と攻撃の多様化【2005年以降】

イラク戦争（2003年～2011年）・アフガニスタン紛争（2001年～継続中）の長期化、BRICs諸国をはじめとする新興国の台頭などにより、相対的に米国の力が低下してきた状況で、国際政治の多極化が進むとともに、2010年以降には、アラブの春、シリア内戦、イスラム過激派組織「イスラム国」の台頭など、中東の政治状況に大きな変化が起きた。東アジアにおいても2006年の北朝鮮のテポドン号発射実験・核実験、南シナ海における中国と周辺国の領有権問題、竹島・尖閣諸島問題などが起きた。

経済的には、2007年のサブプライムローン問題、2008年のリーマンショックの後の世界的金融危機と、長期にわたる世界的な景気後退に見舞われた。景気後退が続く中、我が国では2011年に東日本大震災が発生し、大きな被害を受けた。

この時代は、情報通信技術の分野では、スマートフォンをはじめとするスマートデバイスの普及とクラウド技術の登場が大きなトピックである。

Apple iPhone（2007年米国発売）、Android搭載スマートフォン（2008年米国発売）が発売されると、従来型の携帯電話を上回る売れ行きとなり、日本メーカーが発売していた国内専用の高機

(35)　経済産業省「事業継続計画策定ガイドライン」2005. <http://www.meti.go.jp/report/downloadfiles/g50331d06j.pdf>

能携帯電話端末（フィーチャーフォン）は「ガラパゴス携帯（ガラケー）」などと呼ばれ消滅が危惧されるような状況になっている。

クラウドコンピューティングとは2006年にGoogleのCEOであるエリック・シュミット（Eric Schmidt）が提唱した概念で、データやソフトウェアをネットワーク経由で提供するサービスのことである。従来からネットワーク経由で提供する情報処理サービスは存在しており、必ずしも新しい技術・概念ではないが、広範なサービスを包含する言葉として受容されている。また「ビッグデータ（用語集参照）」や、IoT/M2M[36]などの概念が登場し、利用が活発化してきている。

サイバーセキュリティ分野では、①国家安全保障に影響するような攻撃や秘密情報漏えい事件の発生、②企業の営業秘密の窃取を目的とした攻撃や情報漏えい事件の発生、③重要インフラの制御システムを狙った攻撃、といった特徴的な攻撃・事件等が発生している。

国家安全保障に影響するような攻撃としては、2007年に発生したエストニアへのサイバー攻撃（初の国レベルへの攻撃）、2011年に発生した衆議院・参議院を対象とした標的型サイバー攻撃、2013年に発生した韓国での大規模サイバー攻撃などが代表的なものである。また、秘密情報漏えい事件としては2010年に発生した米国外交公電等がWikiLeaks（ウィキリークス）に流出した事件、2010年の尖閣諸島中国漁船衝突映像が流出した事件、2013年の元NSA・CIA職員のエドワード・ジョセフ・スノーデン（Edward Joseph Snowden）による諜報関連情報の暴露などがある。これらの事件を踏まえ、各国政府は様々な対策を講じている。日本政府においても2013年に策定された「国家安全保障戦略」において、サイバー空間の防護及びサイバー攻撃への対応能力の一層の強化を謳うとともに、2013年に策定された「サイバーセキュリティ戦略」において、国家レベルのサイバー攻撃に対する対応の強化が示されている。サイバー攻撃の脅威に適切に対応するため、2014年には防衛省にサイバー防衛隊が設置された。また、同年には我が国のサイバーセキュリティに関する施策の基本方針を定めた「サイバーセキュリティ基本法」が成立している。

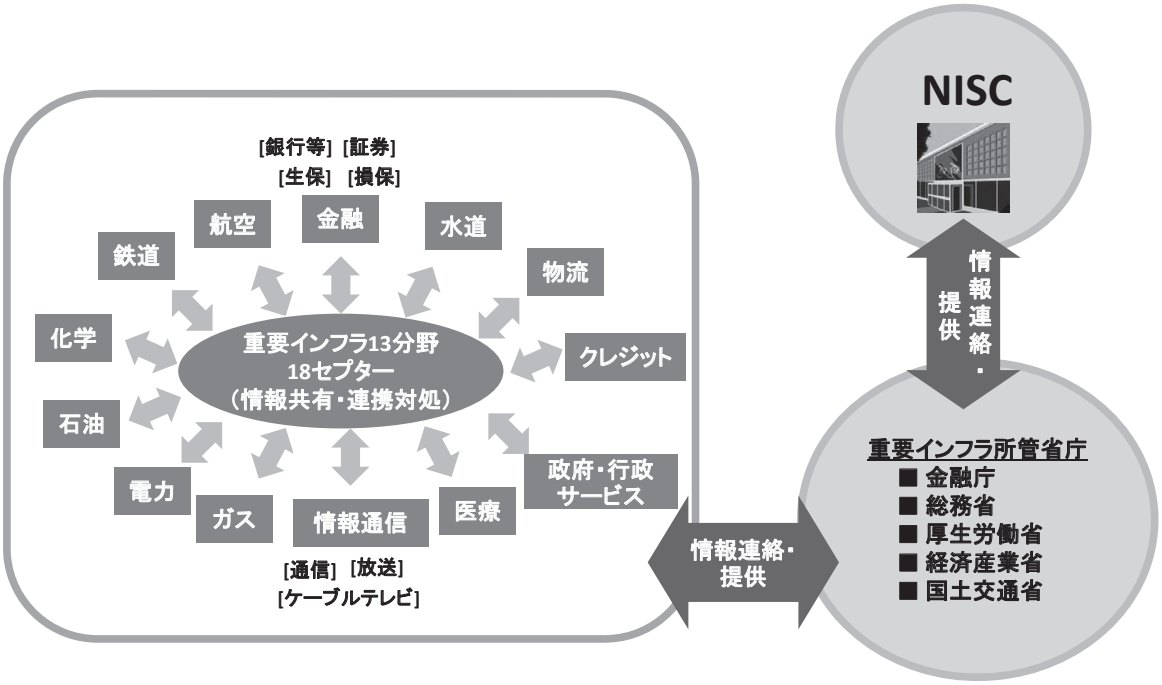
我が国の企業の営業秘密の窃取を目的とした事件としては、2007年のデンソーからの機密データ持ち出し事件[37]、2011年に発生した三菱重工等の防衛関連機器メーカーがサイバー攻撃を受け秘密情報を窃取された事件などがある。これらに対応するため、不正競争防止法の改正により営業秘密侵害罪の罰則強化等が進められてきている。また、情報漏えい事件としては、2011年にソニーがサイバー攻撃を受け約1億件の顧客情報が漏えいした事件や、2014年にベネッセコーポレーションから顧客の個人情報が約3500万件漏えいした事件などがある。これら事件を受けて「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」が改訂される（平成26年厚生労働省・経済産業省告示第4号）とともに、個人情報保護法の改正も検討されている。

重要インフラの制御システムを狙った攻撃としては、2010年のStuxnetと呼ばれる産業制御システムを対象としたマルウェアがある。Stuxnetによりイランの核燃料施設のウラン濃縮用遠心分離機のPLC（Programmable Logic Controller）が改ざんされ、8,400台もの遠心分離機が稼働不能となったとされている。日本においては、制御システムに対するサイバー攻撃の脅威に対応するため、2012年に経済産業省が支援し、民間企業等が組合員として参加する制御システム

(36) M2MはMachine to Machineのことで、人間が介在しない機器間の通信のことを指す。
(37) 逮捕された中国人社員は処分保留で釈放後に懲戒解雇となった。「デンソー　中国人社員を懲戒解雇」『日本経済新聞』2007.4.18, 夕刊.

セキュリティセンター（Control System Security Center: CSSC）が設立された。また、NISCでは2006年から重要インフラにおける分野横断的演習（Critical Infrastructure Incident Response Exercise: CIIREX）を開催している（図6参照）。

図6　NISCによる分野横断的演習（CIIREX）



（出典）内閣官房情報セキュリティセンター「「2013年度重要インフラの分野横断的演習に関する調査」の結果について」2014.3.11, p.3. <http://www.nisc.go.jp/active/infra/pdf/bunyaoudan_2013.pdf>; 内閣官房情報セキュリティセンター「重要インフラにおける分野横断的演習の実施概要について―2014 年度分野横断的演習―」2014.12.9, p.1-2. <http://www.nisc.go.jp/active/infra/pdf/bunya_enshu2014gaiyou.pdf>を基に三菱総合研究所作成。

我が国におけるこのほかの主要な動向として、2011年には「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」（いわゆる「サイバー刑法」。平成23年法律第74号）が成立している。これは、サイバー犯罪条約に対応した国内法の整備として実施されたもので、これにより同条約を批准することとなった。

総論では、調査の概観として、本調査報告書における「サイバーセキュリティ」の考え方や近年の情報通信技術とサイバーセキュリティを取り巻く現状を示した上で、それらを理解する上で重要な歴史的背景を整理した。総論を踏まえ、続く概論ではサイバーセキュリティにかかわる脅威、技術、法制度、社会的側面などの個別分野に関して概況を示す。第Ⅱ部の主要事項は概論の個別分野に対応した形で、各分野において主要な事項について解説するとともに、国内外の事例を紹介する。

執筆：株式会社三菱総合研究所　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）
監修：慶應義塾大学　名誉教授　土居（どい）　範久（のりひさ）