＜研究ノート＞

日本におけるセキュリティ概念の展開
―情報技術の発展と脅威の多様化に関する一考察―

近　藤　　光

要旨

現在，セキュリティという言葉は広く一般に知られるようになった。日本においてこの言葉はしばしば情報技術と関連付けられ，「情報セキュリティ」の意味で用いられている。かつては情報技術を専門とする一部の人々が関心を寄せていた情報セキュリティという言葉に対する認識は，その理解度は別として，社会一般にまで広がっているといえる。

本稿の目的は，日本における「セキュリティ」に対する考え方の変遷を，情報技術の発展，情報に対する脅威，情報セキュリティへの認知と脅威への対応といった点から整理することである。

キーワード

情報セキュリティ，セキュリティ概念，ネットワーク技術，CSIRT，情報共有，事故前提組織

はじめに[1]

近年，情報技術の活用が進み，日々の生活にとって不可欠なものになっている。情報システムは社会を支えるインフラであり，その重要性は増大しているが，それ故に情報システムに対する脅威も高まり続けている。こうした脅威は，

[1] 本稿の「はじめに」は，経営情報学会2015年秋季全国研究発表大会，オーガナイズドセッション「我が国におけるCSIRTの現状と課題」の第1報告「日本における情報セキュリティの歴史的変遷」をベースに加筆・再構成したものである。同セッションについては（寺本ら，2015）を参照のこと。

コンピュータ・ウイルスやフィッシング，DDoS攻撃，不正アクセス，IoT機器を狙ったサイバー攻撃などさまざまであり，時代とともに変化してきた。

現在，日常において「セキュリティ」という言葉を用いる時，その多くは自然と「情報技術」と関連付けられ「情報セキュリティ」の意味で用いられている。かつては，研究者，技術者，あるいは企業・政府の情報システム担当者など情報技術を専門とする一部の人々が関心を寄せていた情報セキュリティという言葉に対する理解は，その濃淡は別として，社会一般にまで広がっているといえるだろう。

情報システム分野で「セキュリティ」という言葉が使われるようになったきっかけは，1960年代後半に米国ランド社の研究が公表されたことであると考えられる。日本でも1980年代になるとパソコン通信を介したコンピュータ・ウイルスが発見されるなど，情報セキュリティに関心が寄せられた。しかし，当時はセキュリティという言葉はさほど浸透していなかったと考えられる。その後，1990年代のインターネットの普及により，ネットワーク利用者が増加し，そこで扱われる情報の種類と量，それに対する脅威も多様化していった。この変化を受けて情報セキュリティが扱う領域は拡大し，ネットワーク，そして個人利用者へと対象を広げていった。このネットワークの拡大と情報システムの利用者増加の影響は大きく，政府や企業におけるセキュリティへの認知と取り組みに変化をもたらした。

本稿の目的は，日本において「セキュリティ」という概念の変遷を，情報技術の発展，情報に対する脅威，情報セキュリティへの認知と脅威への対応といった点から整理することである。

次節以降，（1）情報技術の発展と脅威の多様化，（2）「セキュリティ」概念の広がりと変化，（3）新たな可能性としてのCSIRT，と議論を進めていく。（1）では情報技術の発展によってどのように脅威が変化していったのかを明らかにする。そこでは，技術が発展するがゆえに脅威の種類と対象が多様化していったことが明らかになる。（2）では「セキュリティ」という言葉が情報分野だけ

でなく，社会においてどのように受け取られていったのかを（1）と関連付けながら考察していく。そして（3）では，こうした変化を受けて現代企業に突きつけられている課題とその解としてのCSIRTの可能性について述べるとともに，今後の課題を示す。

1．情報技術の発展と脅威の多様化

1－1．技術発展と脅威の関係

情報セキュリティとは一般的には，「情報の機密性，完全性および可用性を維持すること」とされる[2]。本稿の目的の中心はセキュリティに対する考え方，「セキュリティ概念」の変遷を明らかにすることであるが，まず本節で情報技術の発展と脅威の多様化について整理したい。

情報を守るための手段は，コンピュータが発達しＩＴ技術が広く普及する遥か前から存在していた。その代表例が「暗号（化）」である。現存する最古の暗号としては古代エジプト時代，石碑に刻まれたヒエログリフ（象形文字）が知られており，これは紀元前1800年頃まで遡る[3]。そこで用いられている暗号は換字式暗号（substitution cipher）の最も初期の例であるが，やがてより複雑な暗号が考え出されるようになった。当時は守るべき情報は物理メディアに直接記述されており，脅威はそれ自体を盗まれたり，盗み見られたりすることで機密情報が流出することであったといえる。

暗号化は情報を特定の相手以外に読み解かれないようにするための手段であるが，電信技術，無線技術，コンピュータ，MPU，インターネットなど，新しい技術の誕生によって状況が変化していく。情報を守るための手段も高度化する一方，それら技術を利用した新たな脅威が生まれたからである。

---

[2] 情報セキュリティマネジメントシステムに関する国際規格「ISO/IEC27001：2013」による。

[3] Cypher Research Laboratories社Webページ，*A Brief History of Cryptography*，（http://www.cypher.com.au/crypto_history.htm）2022年３月８日アクセス。

例えば，無線技術によって離れた相手と直接情報をやりとりできるようになったが，無線を第三者によって傍受されるという新たな脅威が生まれた。利用者からすると，無線が傍受されたことを察知することは困難であり，そのため高度な暗号技術の必要性を高める結果となった。

半導体技術の発展によって，コンピュータの計算能力が向上するとともに，複雑な暗号技術の利用も可能になったが，一方で，暗号解読の技術にも活用されることになった。コンピュータが広く普及していったことは，利便性向上というプラスの面だけではなく，利用者の増加による攻撃対象の拡大と攻撃者そのものの増加という問題も生じさせたと考えられる。

コンピュータやPCといった情報通信機器の発展，さらにネットワーク技術の発展によってコンピュータ・ウイルスが多く作成されるようになり感染が拡大していく。情報技術の発展は利便性の向上をもたらすと同時に，それに対する脅威も増大させている。なかでも，インターネットの普及によって個人利用者が増加したことは，脅威の種類と質を大きく変化させたといえる。そこで，インターネット以前と以後に分けて整理する。

1－2．インターネット以前

先述した通り，情報への脅威とその対応は紀元前まで遡ることができるが，その後の技術革新によって情報セキュリティを取り巻く環境は大きく変化してきた。特に，電信・無線といった通信技術とコンピュータは大きな影響を与えたと考えられる[4]。前者は1830年代から実用化が進み，後者は1940年代から発展を遂げた[5]。

4　現代の「情報セキュリティ」という考え方はこれらの技術が発展した後に形成されていったと考えられるが，de Leeuw（2007）は，17世紀後半，フランスとオランダの戦争を回避するために活躍したフランスの外交官Jean-Antoine de Mesmes の活動に現在の情報セキュリティ概念との類似性が見られると指摘している。詳細は同文献を参照。

5　中野（2017）によれば，1794年にはフランスのパリからリールまでの約200kmを結ぶ腕木通信（semaphore）が運用されているが，この方式は電気を用いたものではな

通信技術はそれまで不可能だった遠隔地との情報のやりとりを可能にするため，即時に状況を把握する必要がある軍事は当然のこと，規模が拡大し遠隔地の管理を必要とする民間企業にも利用されていった[6]。これら通信技術は有線から無線へと発展していったが，それに伴い傍受されるリスクが増大した。また，有線・無線を問わず通信が作戦（業務）遂行上の重要な要素となると，相手方の情報獲得だけでなく通信そのものを妨害するという情報システムに対する脅威も顕在化していったと考えられる[7]。日本においては，1869年に東京と横浜の間で電信が開始され，1871年には国境を越えての国際通信が可能になった[8]。

一方，コンピュータについては1940年代に軍用を中心に開発が進んだ。初期の代表的な機種として，1941年のアタナソフ&ベリー・コンピュータ（ABC），1946年のエニアック（ENIAC）が知られている。両機はアメリカで開発されたものであるが，イギリスでも1943年にコロッサス（Colossus）が開発されている。コロッサスはドイツ軍の暗号解読用に開発されたものであり，それ以前の機械式解読機では解読までに時間がかかりすぎるために生み出された[9]。

いため，電信には含まれない。また，腕木通信は電信が発達すると衰退していったという。なお，電信に関しては1837年にアメリカのモースが電磁式電信機を発明し，後にMagnetic Telegraph Companyを創立している。

[6] 例えばアメリカの鉄道会社のひとつエリー鉄道では度重なる事故の削減のため，1851年に電信による運行管理を導入した（近藤，2007）。

[7] 1914年，第一次大戦において，イギリスはドイツの海底ケーブルを切断することで通信を妨害した。結果としてドイツはイギリスを経由するケーブルを使用することとなり，通信の暗号化を迫られたという。HH News & Reports「【第 4 回】無線の登場と情報戦～第1次世界大戦の暗号解読～」（https://www.hummingheads.co.jp/reports/series/ser01/110616.html）2022年 3 月10日アクセス。

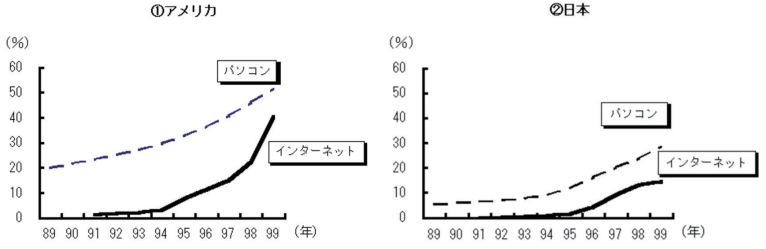
[8] 大野（2018）によれば，1871年にデンマークの通信会社が長崎～上海，長崎～ウラジオストク（ロシア）間をつなぐ長距離海底電信ケーブルを敷設したとされる。また，次の文献も参照のこと。TIME&SPACE「【国際通信150年 (1)】はじまりは明治時代！約1,000kmの海底ケーブル敷設方法は？通信料は？」（https://time-space.kddi.com/au-kddi/20210825/3160）2022年 3 月 8 日アクセス。

[9] Coombs,1983.

他方，商用のコンピュータは1950年代から，UNIVAC1をはじめとして，各メーカーが様々な機種を発表，徐々に市場に受け入れられ，IBMが1964年に発表したシステム360は業界に大きな影響を与えた。同機は翌年には日本で発売され，日本の総合電機メーカーもコンピュータ開発を積極的に進めた。

その後，1970年代にはパーソナルコンピュータ（PC）が発売された。PCは当初は価格も高く機能も限定されており，業務用を除けばマニアが購入するものであった。しかし，日本とアメリカでは普及のペースに違いはあるものの，次第に普及率は上昇していった[10]。1984年にはMacintoshが発売，1992年にはWindows3.1が発売，1995年にはWindows95が発売されている。なお，日本では1993年にインターネットの商用利用がスタート[11]したが，PCを利用した通信サービスとして1980年代半ばからパソコン通信が普及し始めた。パソコン通信はインターネットとは異なり，各サービスの会員限定の環境ではあったが，個人がネットワークを利用する契機となった。

図表１　日本とアメリカにおけるパソコンとインターネットの普及率



（出所）ＩＴＵ"Yearbook of Statistics 2000, Chronological Time Series 1989-1999"、ＯＥＣＤ Databaseより作成。

原　出　所：ITC “Yearbook of Statistics 2000, Chronological Times Series 1989-1999”, OECD Database.
出所：内閣府Webページ，「平成12年度年次世界経済報告」
（https://www5.cao.go.jp/j-j/wp-we/wp-we00/sekaihakusho-00-16.html）

[10] PCやインターネットの普及率についてはデータによって違いがあるが，内閣府の「消費動向調査」によれば1989年のＰＣ普及率は11.6%，1995年は15.6%であった。

[11] 日本ではIIJが1993年11月にサービスを開始した。なお，学術目的では1980年代からインターネット利用が行われているが，本稿では1993年をインターネットの開始とした。

以上，この時期の特徴を整理すると，まず，当初は通信技術やコンピュータの利用は軍用などに限られ，利用側も攻撃側も専門的な知識を持った人間に限られていたということである。攻撃の理由も戦況を有利に進める，相手の行動を妨害するといった明確な意図を持っていたと考えられる。しかし，次第にコンピュータの業務利用が広がり，さらにPCの普及によって個人の利用者が増えていくことで状況が変化していった。すなわち，かつてほど専門的知識をもっているわけではない個人がPCを所有し，パソコン通信という限定された環境とは言え，ネットワークに繋ぐ事例も増えてきたということである。また，その間，企業におけるPCの導入は進み，日常の業務で利用される機会が増え，企業における情報システムの重要性が増大していったと推察される。ただし，日本では個人も企業も多くは外部のインターネットに接続されてはおらず，脅威については限定的であったといえるだろう。後述するように，1988年にはパソコン通信（PC-VAN）内でコンピュータ・ウイルスが発生するなどの問題はあったが，海外の様に大規模なインシデント[12]が発生していたわけではなかった。コンピュータ・ウイルスは当時のセキュリティ上の重大な脅威ではあるが，その感染の経路は限られていたほか，その内容も何らかのメッセージを表示させるかファイルを削除するといった単純なものであったとされる[13]。

1－3．インターネット以後

インターネットの普及率は急速に拡大し，2002年には50％を越えて近年は80％台を示している。この間もネットワークに関する技術とPCの性能は向上し，さらにスマートフォンの普及も進むなど，多くの情報がネットワークを介

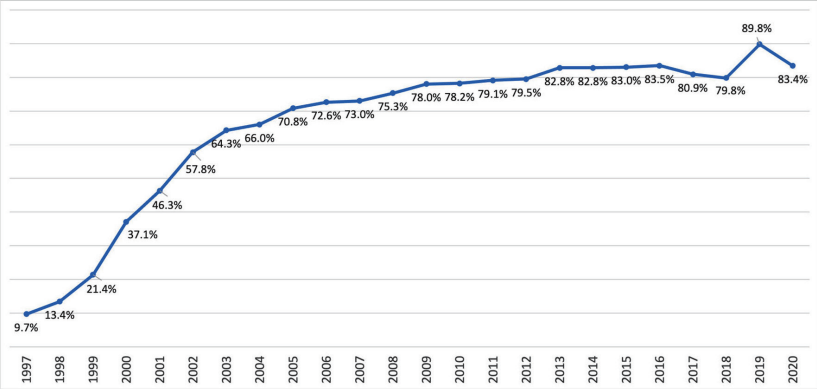
---

[12] 1988年にモリスワームといわれるプログラムがインターネット上に放たれて当時インターネットに接続していた多くのコンピュータがほぼ使用不能になった。詳しくは，JPCERT/CC「インターネットセキュリティの歴史 第1回「Morris ワーム事件」（https://www.jpcert.or.jp/tips/2007/wr071202.html）2022年3月9日アクセス。

[13] G DATA「ウイルスの歴史」（https://www.gdata.co.jp/labs/history）2022年3月15日アクセス。

してやり取りされるようになっていった[14]。これほど高い普及率になると，専門的知識をもっている利用者の方が少数となり，それ以前とは根本的に異なる状況にあるといえる。

図表２　インターネットの人口普及率（1997年～ 2020年）



注：2019年は調査票の設計が例年と異なっているため，その数値の扱いには注意を要する。
出所：総務省「通信利用動向調査」より作成。

インターネットの普及に合わせて，2000年以降には攻撃手法が多様化していった。インターネット普及以前は，攻撃の経路も限られ，PCを保有していない世帯も多いなど，その脅威は限定的であった。しかし，インターネットの普及はPCの普及を促した。攻撃者から見た場合，利用者の増加は攻撃対象の広がりと捉えられ，これが脅威の目的と手法の多様化へとつながった。さらに，ブロードバンドの普及でPC起動中は常時接続が当たり前となり，モバイル端末においてもスマートフォンが普及したことで，多くの個人情報を記録した端

[14] iPhoneでは第２世代にあたるiPhone 3Gが2008年６月９日に日本でも発売された。詳しくは，ITメディアWebページ，「iPhoneを振り返る」（https://www.itmedia.co.jp/mobile/articles/1708/10/news036.html）2022年３月９日アクセス。

末が常にネットに接続されるようになった。結果，社会的・政治的な主張を目的とするハクティビスト，ネット上でのスパイ活動，マルウェアの流行，フィッシング（Phishing）詐欺など脅威は多様化し，政府や企業だけでなく個人までがその対象となった。

日本におけるセキュリティ上の脅威を整理するため，ここではIPA（情報処理推進機構，以下IPAと表記）の資料を利用する。IPAは毎年，「情報セキュリティ 10大脅威」を発表している。図表 3 は「情報セキュリティ 10大脅威 2022」として発表されたものである。個人部門では個人情報の詐取，ネット上の誹謗・中傷・デマ，メールやSMSによる脅迫・詐欺の手口による金銭要求と続き，組織部門ではランサムウェアによる被害，標的型攻撃による機密情報の窃取，サプライチェーンの弱点を悪用した攻撃となっている。

図表 3　情報セキュリティ 10大脅威 2022

■「情報セキュリティ10大脅威 2022」　　NEW：初めてランクインした脅威

昨年順位	個人	順位	組織	昨年順位
2位	フィッシングによる個人情報等の詐取	**1位**	ランサムウェアによる被害	1位
3位	ネット上の誹謗・中傷・デマ	**2位**	標的型攻撃による機密情報の窃取	2位
4位	メールやSMS等を使った脅迫・詐欺の手口による金銭要求	**3位**	サプライチェーンの弱点を悪用した攻撃	4位
5位	クレジットカード情報の不正利用	**4位**	テレワーク等のニューノーマルな働き方を狙った攻撃	3位
1位	スマホ決済の不正利用	**5位**	内部不正による情報漏えい	6位
8位	偽警告によるインターネット詐欺	**6位**	脆弱性対策情報の公開に伴う悪用増加	10位
9位	不正アプリによるスマートフォン利用者への被害	**7位**	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	NEW
7位	インターネット上のサービスからの個人情報の窃取	**8位**	ビジネスメール詐欺による金銭被害	5位
6位	インターネットバンキングの不正利用	**9位**	予期せぬIT基盤の障害に伴う業務停止	7位
10位	インターネット上のサービスへの不正ログイン	**10位**	不注意による情報漏えい等の被害	9位

注：このランキングは2021年に発生した情報セキュリティに関する事案からIPAが脅威候補を選出したうえで，「10大脅威選考会」によって審議・投票されたものである。
出所：https://www.ipa.go.jp/security/vuln/10threats2022.html

この「10大脅威」の発表は2006年からはじまったものであるが，当初のランキングでは個人と組織を分けて掲載していなかった。それが2015年から個人と組織に分けて作成されている。同ランキングについては，2019年にIPAの研究員である黒谷欣史氏が①「05 ～ 09年」，②「10年～ 14年」，③「15年～ 18年」の 3 つに時期区分した上で，次の点を指摘している[15]。

まず①の時期から，現在まで続く脆弱性を狙う攻撃が脅威の多くを占めていたということである。これについてはランキングが作成される以前，1990年代から見られた傾向としている。また，ファイル共有ソフト（Winnyなど）の利用からマルウェアに感染し，個人や企業の情報が漏洩するケースが増えたのもこの時期である。

次いで，②の時期に入ると，スマートフォンを標的として脅威が増大していく。スマートフォンを狙う不正アプリはインターネットバンキングの普及を背景にしているという。

最後に③の時期からは，ランサムウェアによる被害が見られるようになった。これはビットコインをはじめとする仮想通貨の普及が要因であるとしている。加えて，IoT機器を狙うウイルスが登場し，実際に被害を及ぼすケースも出てきたとされる[16]。

---

[15] ITメディアWebページ「14年分の「情報セキュリティ 10大脅威」を振り返り“変わらない” 5 つの対策」（https://www.itmedia.co.jp/news/articles/1905/29/news020.html）2022年 3 月21日アクセス。2019年 5 月開催の「第16回 情報セキュリティEXPO」での講演によるもので，2018年までのランキングをもとにされている。

[16] IoT機器を標的としたマルウェア「Mirai」が2016年に様々なWebサービスをアクセス困難にした。詳細は次の資料を参照。「顕在化したIoTのセキュリティ脅威とその対策」（https://www.ipa.go.jp/files/000059579.pdf）2022年 3 月 9 日アクセス。

以上，黒谷氏の指摘をまとめたものであるが，利用者と利用サービスの増加といった社会の変化がきっかけとなり脅威が多様化していることが伺える。例えば，①の時期におけるファイル共有ソフトの利用によるマルウェアの感染は，専門的な知識をもったユーザーが中心であったころならば大きな脅威とならなかったかも知れない。しかし，インターネットが誰でも手軽に使えるようになることで大きな脅威となった。また，個人のPCが感染することで個人の情報だけでなく，企業の情報までが漏洩してしまったことは，企業が従業員に対して機密情報を個人所有のPCに保存することを制限するなど，情報セキュリテイ上の対応を求めることにつながった。②の時期から増加しているスマートフォンを対象とした脅威は，端末自体の性能向上（フィーチャーフォンからスマートフォンへの変化）という技術的な要因と，金融をはじめとした様々なサービスがウェブ上で展開されるようになった事がもたらしたものである。この時期から明確に金銭的な目的によって組織的な攻撃が行われるようになったといえる。③の時期から現在までをみると，仮想通貨の流行とそれに対するランサムウェアの増加，2022年のランキングにあるようにテレワークなど新しい生活様式を対象とする脅威など手口は多様化を続けているといえる。

以上の点をまとめると，新たな技術の普及やサービスの展開といった社会の変化が脅威を増加・多様化させるということが指摘できる。利用者の増加は各種サービスにとって多くの恩恵をもたらすが，セキュリティという点においてはリスクを増大させるといえる。一方で，セキュリティ対策の重要性は，IPAなど専門機関による活動や報道，企業など組織内での取り組みによって認知されるようになってきたともいえる。このセキュリティという概念について次節で整理する。

「セキュリティ」概念の広がりと変化

情報セキュリティの定義としてよく用いられるのは，「情報の機密性，完全性および可用性を維持すること」（ISO/IEC27000：2013）であり，機密性：

Confidentiality，完全性：Integrity，可用性：Availabilityといわれるセキュリティの 3 原則で説明される。

セキュリティに関連する言葉として主に情報セキュリティ（Information Security）とコンピュータ•セキュリティ（Computer Security）があるが，グーグルのNgram Viewerでその出現頻度を示すと図表 4 の通りとなった。1970年頃まではどちらの用語も出現頻度は低く大きな差はなかったが，その後はコンピュータ・セキュリティという用語が優位にあるのがわかる。しかし，1990年代以降コンピュータ・セキュリティの出現頻度は低下し，代わりに情報セキュリティの出現頻度が増加していった。これは，インターネットの利用増加などが関連していると推察される。なお，日本語についてはNgram Viewerの対象外であるため，各社の新聞記事から情報通信分野やコンピュータに関連して「セキュリティ」という言葉が使われているケースを調査した。日経産業新聞では1975年 4 月「コンピューターサービス，セキュリティ事業部を新設――電算機の“安全保障”探る」という記事が掲載されている[17]。読売新聞では1982年 2 月の「コンピュータ犯罪防止は従業員信頼で」という記事が最も古く[18]，朝日新聞では1983年12月の産業構造審議会による通信制度見直しの提言に関する記事において，「コンピュータ・セキュリティ（安全保障）」という言葉が使われていることが確認できた[19]。それ以前も「セキュリティ」という言葉は使われているが，警備，国家安全保障，証券，エネルギーなどに関連した使用であった。以上のことから，一般紙では1980年代から，専門誌ではそれより先行して1970年代なかばには「セキュリティ」が現在の意味に近いかたちで用いられ始

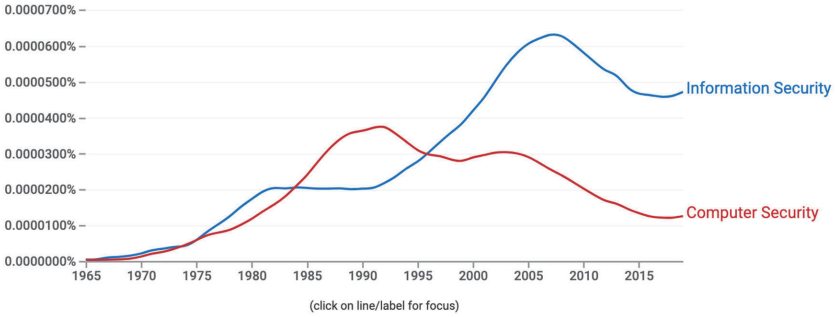
[17] 「コンピューターサービス，セキュリティ事業部を新設――電算機の“安全保障”探る」『日経産業新聞』，2 面。なお，日経四紙（日経・産業・流通・金融）を日経テレコンから検索しているため，検索可能な記事は1975年以降である。このため1975年より前にも関連記事がある可能性は否定できない。なお，朝日新聞は1879年以降，読売新聞は1874年以降の記事から検索している。

[18] 「コンピュータ犯罪防止は従業員信頼で」『読売新聞』1982年 2 月25日，朝刊，8 面。

[19] 「通信制度見直し提言　電算機の保安対策も」『朝日新聞』1983年12月 1 日，東京，朝刊，9 面。

めたと推察される。

図表 4　Information SecurityとComputer Securityの出現頻度の比較（1965年～ 2019年）



注：Ngram ViewerはGoogle Booksのテキストコーパスを検索し，検索語の出現頻度を示したものである。
出所：Google Books Ngram Viewer。

そもそもコンピュータや情報システムといった専門的な領域において，セキュリティという言葉が使われるようになったのはいつ頃からだろうか。名和（2005）は，Wareによるランド研究所（RAND Corporation）におけるコンピュータ・システムの脆弱性に関する研究（Ware,1970，以下，『ランド報告』）を挙げている[20]。

『ランド報告』では「コンピュータ・システムのセキュリティを支える基本的な原則は，全システムを隔離された物理的環境のなかに移すことである。そこでは外部からの侵入は，その影響が許容水準に収まるように最小化されなければならない」としている（Ware, 1970，名和，2005）[21]。

この報告における「セキュリティ」は，世界をシステムの「外と内」に分けることが前提であり，その上でセキュリティの問題を①コンピュータに格納さ

[20] Willis Wareは『ランド報告』に先立ち1967年にもSpring Joint Computer Conferenceにおいて，Security and Privacy in Computer Systemsという報告をしている。
[21] 日本語訳については名和（2005），p.22による。

れた秘匿情報の保護，②各ユーザーが他のユーザーの干渉を受けないという 2 つに分類していることが指摘されている（名和，2005）。この『ランド報告』の公表を契機に，情報システム分野でセキュリティという言葉が普及したが，当時はセキュリティが扱うべき対象は，「コンピュータの中にある情報」に限定されており，さらに当時のコンピュータは限定された人々によって利用され，限られたネットワーク内で稼働していたといえる。

『ランド報告』をきっかけに「セキュリティ」という言葉が注目を浴びたといえるが，日本では「セキュリティ」という言葉はどのように理解されていったのだろうか。名和（2005）によると，1970年時点で日本アイ・ビー・エムはセキュリティを「機密保護」と訳しているが[22]，それから時を経た1988年においても，セキュリティという言葉について適訳がないと言及されている[23]。

一方1988年といえば，先述したようにアメリカを発端にインターネット上でモリスワームが広がり，日本でもパソコン通信においてコンピュータ・ウイルスである「PC-VANウイルス」が発見された年である。このような現実的な脅威が発生することでセキュリティの概念が発展していく。日本では，1990年に通産省が「コンピュータウイルス対策基準」を策定した[24]。

セキュリティに関する関心と定義に特に大きな影響を与えたのが，1992年にOECDが『情報システムのセキュリティに関するガイドライン』（OECD Guidelines for the Security of information Systems）を策定したことである。同ガイドラインにおいて，情報セキュリティとは，「所謂 CIAの欠如に起因する危害から情報システムを利用するユーザを守ること」と定義された[25]。この

---

[22] 名和（2005），p.23。現出典は日本アイ・ビー・エム（1970）『情報処理用語』，p.201。

[23] 千葉（1988），p.638。

[24] IPAは1970年に設立されたが，1990年の「コンピュータウイルス対策基準」（通商産業省告示 第139号）によってIPAがコンピュータウイルスを発見した者が被害の拡大と再発を防ぐために必要な情報を届け出る唯一の公的機関として指定された。IPAのWebページを参照。（https://www.ipa.go.jp/security/outline/outline-j.html）2022年 3 月 9 日アクセス。

[25] OECD, “OECD Guidelines for the Security of Information Systems, 1992”

OECDのガイドライン発行後，「情報セキュリティ（information security）」を冠したガイドラインや法律が整備されていった[26]。日本においても，これらのガイドラインは参照されつつも，1995年の通産省による「情報システム安全対策基準」のように，長い間「セキュリティ」は安全と理解されているように見受けられる。

前節で示したように1990年代にはインターネットの商用利用が開始され，日本においても急速に利用者が増加した。商用利用開始から 5 年後の1998年には日本のインターネット利用者は1000万人を突破したと考えられている[27]。

インターネット利用者の増加とそれによる脅威の発生は情報セキュリティに対する関心を急速に増大させたと考えられる。特に2000年以降の様々なセキュリティ上の事故が発生したことは関心を高めるきっかけとなり，セキュリティ概念が一般に知られる契機となった（主な事故は図表 5 を参照）。

OECDは2002年に“the Security of Information Systems and Networks: Towards a Culture of Security”としてガイドラインを改定している[28]。そこでは，セキュリティ文化という概念を提唱，通信手段の多様化を反映，1992年版では「政府や企業」が主な対象だったが，「政府，企業，その他の組織および個人利用者」と改め，これを参加者（participants）と呼び，参加者すべてが情報セキュリティに責任を負うと規定するなど大きな変更が行われている。新ガイドラインでは，「情報セキュリティの必要性，セキュリティの強化のた

（https://www.oecd.org/sti/ieconomy/oecdguidelinesforthesecurityofinformationsystems1992.htm）2022年 3 月 9 日アクセス。

[26] 例えば，BSI（英国規格協会）による「情報セキュリティに関するガイドライン」“BS7799”（1995年）や，ISO/IECによる「情報セキュリティガイドライン」“15408”（1999年）など。

[27] 国立国会図書館調査及び立法考査局（2014），p.15.

[28] OECD，“OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security”（https://www.oecd.org/sti/ieconomy/oecdguidelinesforthesecurityofinformationsystemsandnetworkstowardsacultureofsecurity.htm）2022年3月9日アクセス。

めに参加者ができることを認識すること」が求められており,「参加者は,セキュリティの事件に対する予防，検出及び対応のために，時宜を得たかつ協力的な方法で行動すべきである」としている[29]。それを実現するための方策の１つが「脆弱性，インシデントの情報提供」であり，次節で扱うCSIRTの役割が注目されるようになる。

以上，本節ではセキュリティ概念の変化をガイドラインの変化によって確認した。前節でみたように，利用者の増加によって脅威の対象が広がり，その手口も多様化していった。このことは社会におけるセキュリティへの認知を高め，それを反映する形でOECDなどによるガイドラインなども変更されていったのである。2002年のOECDによる新ガイドラインは，情報セキュリティの対象が個人まで広がっていくという現実を反映させたものであるといえる。

図表５　事故の発生とセキュリティ対応

セキュリティ事故	CSIRTの設立	政策
2001-2003年 ・情報漏洩事故の発生 ・Nimdaの流行	2001年 IIJ-SECT	2001年 ・e-Japan戦略 ・情報セキュリティに関する専門家会議（IPA主催）
2003-2004年 ・情報漏洩事故の発生 ・“ブラスター”の流行	2003年 JSOC, NTT-CERT 2004年 KLIRRT, SBCSIRT	2003年 ・情報セキュリティ総合戦略の策定
2005年 ・情報漏洩事故の発生 ・スパイウェア、フィッシング詐欺の流行 ・Winnyによる情報漏えい事故	2005年 KDDI-CSIRT	2005年 ・内閣官房情報セキュリティ センター(NISC) （2014年、内閣サイバーセキュリティセンターに改組）

出所：日本シーサート協議会Webページなど各種資料をもとに筆者作成。

おわりに：新たな可能性としてのCSIRT

以上の内容を整理すると，(1) 暗号技術からはじまり，かつてはごく限られた領域で扱われていたセキュリティという「問題」は，情報通信機器の普及と特

[29] IPA,「新OECD情報セキュリティ・ガイドラインの概要」（https://www.ipa.go.jp/security/fy14/reports/oecd/handout.pdf）2022年３月11日アクセス。

にインターネットの普及によって個人にまで広がっていったこと，(2) セキュリティという言葉も情報技術の発展によって一般にまで浸透したこと，(3) 脅威の多様化を受けて，各種ガイドラインや政策は改正されているが，対象の広がりもあって「セキュリティ」が示す意味は広く曖昧なものへと向かっていること，(4) 専門家が中心的な利用者であった時代とは異なり，誰もが端末を利用する現在では，セキュリティに対する各自の能力にも大きな隔たりがあること，(5) OECDガイドラインでは，参加者が情報セキュリティの重要性を認識し，情報共有を進める必要性が強調されていること，などが明らかになった。

情報インフラの利用がビジネスの前提となった結果，セキュリティ対応を行う人員そのものが，セキュリティ技術を十分に有していないケースが生じている。そのような制約下で適切な対応を行うための試みとして注目されるのがCSIRTである。

CSIRT（Computer Security Incident Response Team）は「事故は必ず起こるものである」という前提に立って構築され，活動している（近藤ら，2018)。CSIRTはコンピュータセキュリティにかかるインシデントに対処するための組織の総称であるが，設立数の増加はセキュリティ上の脅威が特別なものでなくなったことを反映したものといえるだろう（図表 6 参照)。

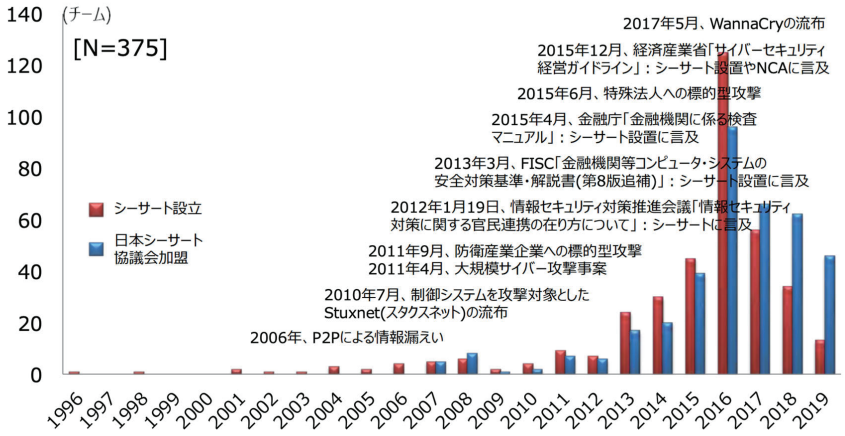
日本シーサート協議会は2007年に設立されたが，その設立趣意書[30]によれば，インシデント対応にこれまでのように単独のCSIRTであたるには限界があり，複数の組織間で情報を共有し協調して立ち向かう必要性，協力関係構築の必要性が高まっていることが示されている。

以上，本研究は日本におけるセキュリティ概念の変遷について総論的に論じたが，今後より詳細な検討が必要であろう。例えば，セキュリティに対する認識は個人と組織によっても、それぞれの専門性や立場によっても大きく異なるはずである。特に企業はセキュリティ対応に迫られ，組織内にCSIRTを構築

[30] 日本シーサート協議会，「設立趣意書」（https://www.nca.gr.jp/outline/prospectus.html）2022年 3 月30日アクセス。

しているが，CSIRTやそれ以前のセキュリティ対応組織が，これまでどのようなセキュリティ上の脅威に，どのように対応してきたのかを明らかにすることが求められる。個別のケースを収集し分析することによって，企業側からみたセキュリティ概念の変遷を明らかにするとともに，脅威が常に変化していくなかで，企業がどのような課題を抱えているのかを継続的に調査していく必要がある。

図表 6 CSIRT設立数の推移（2019年 8 月末まで）



出所：日本シーサート協議会（2019），「加盟組織一覧」，p.16。

附記　本稿は科学研究費基盤研究（B）研究代表者：中西晶「これからの組織に求められる危機への対応とレジリエンス：高信頼性組織論の視点から」（研究課題/領域番号20H01543）による成果である。

文献一覧（Web文献は注に記載）

Coombs, A. W. “The making of Colossus”, *Annals of the History of Computing*, 5 (3), 253-259, 1983.

de Leeuw, Karl Maria Michael, and Jan Bergstra, eds., *The history of*

information security: a comprehensive handbook, Elsevier, 2007.
Ware, W. H., “Security and privacy in computer systems”, *In Proceedings of the April 18-20, 1967, spring joint computer conference*, 279-282, 1967.
Ware, W. H., *Security controls for computer systems*, RAND CORP SANTA MONICA CA, 1970.
大野哲弥（2018）「通信の世紀―情報技術と国家戦略の一五〇年史―」新潮社。
鬼塚史朗（2007）『通信の歴史：理科電話の実験的考察』東京図書出版会。
国立国会図書館調査及び立法考査局（2014）『情報通信技術の進展とサイバーセキュリティ』。
近藤喜代太郎（2007）『アメリカの鉄道史』成山堂書店。
近藤光（2015）「日本における情報セキュリティの歴史的変遷」，経営情報学会2015年秋季全国研究発表大会報告資料（2015年11月28日）。
近藤光, 寺本直城, 杉原大輔, 中西晶 (2018),「CSIRT におけるレジリエンスの罠 日本における現状と課題」,『日本情報経営学会誌』, 37(3), 27-48。
情報処理推進機構『情報セキュリティ白書』各年版（2006 ～ 2021）。
情報処理振興事業協会 セキュリティセンター（2003),「OECD 情報セキュリティガイドライン見直しに関する調査」。
千葉利宏（1988）「高度情報化社会［第 7 回］:高度情報化とセキュリティ」『情報管理』31(7), 627-638。
寺本直城, 杉浦芳樹, 林郁也, 矢寺顕行, 福本俊樹, 近藤光, 杉原大輔（2015）「我が国における CSIRT の現状と課題」,『経営情報学会 全国研究発表大会要旨集2015年秋季全国研究発表大会』57-60。
中野明（2017）『IT全史：情報技術の250年を読む』祥伝社。
名和小太郎（2005）『情報セキュリティ』みすず書房。
日本シーサート協議会（2016）『CSIRT:構築から運用まで』NTT出版。
日本シーサート協議会（2019）「加盟組織一覧」（https://www.nca.gr.jp/imgs/nca_teams_2019.pdf）2022年 3 月30日アクセス。

（こんどう　ひかる　本学非常勤講師）