国立国会図書館

調査と情報―ISSUE BRIEF―

No. 1078（2020. 1. 9）

サイバーセキュリティ政策の現状

キーワード：サイバーセキュリティ、情報セキュリティ、IoT、サイバー犯罪、サイバー攻撃

● 日本におけるサイバーセキュリティ政策は「IT 基本法」が成立した平成 12 年頃から始まり、内閣官房情報セキュリティセンターの設置（平成 17 年）、「サイバーセキュリティ基本法」の成立（平成 26 年）などを経て発展してきた。

● サイバーセキュリティ基本法に基づき設置された「サイバーセキュリティ戦略本部」、「内閣サイバーセキュリティセンター（NISC）」を中心に関連 5 省庁（総務省、経済産業省、警察庁、防衛省、外務省）等がサイバーセキュリティ政策を担っている。

● 日本のサイバーセキュリティ体制は、国際機関等から一定の評価を受けている一方、組織体制、人材育成等に関する課題が指摘されている。

国立国会図書館 調査及び立法考査局
国土交通課　神足（こうたり） 祐太郎（ゆうたろう）

第１０７８号

はじめに

日本では、個人のインターネット利用率は約 8 割[1]、企業における情報通信技術（ICT）の利用率は約 7 割に上るとされる[2]。また、電気、ガス、水道から公共交通、政府機関に至る公共インフラの多くにおいても ICT が利用されており、今や、情報機器・ネットワークは、経済・社会のあらゆる局面に浸透しているといえる。政府は、サイバー空間[3]と現実空間が融合した「Society 5.0」[4]を提唱しており、情報機器・ネットワークと経済・社会の関係は、ますます強まると考えられる。このような状況の中、サイバー空間の安全は現実空間の安全と密接に関係するようになっており、秘匿すべき情報（個人情報等）の漏えいや、システムの改ざんによる現実社会への影響（公共交通網の麻痺等）のリスクが懸念され、対策が課題となっている。本稿では、政府のサイバーセキュリティ政策の経緯と現状を概観する。

Ⅰ　サイバーセキュリティの定義と関連施策の経緯

1　サイバーセキュリティの定義

「サイバーセキュリティ基本法」（平成 26 年法律第 104 号。以下「基本法」）において、サイバーセキュリティとは、①電磁的方式によって記録、伝送等が行われる情報の漏えい、滅失又は毀損の防止等の安全管理上必要な措置、②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確保のために必要な措置が講じられ、維持管理されている状態をいうと定義されている（第 2 条）。

一方、従来の「情報セキュリティ」は、「可用性（Availability）、機密性（Confidentiality）、完全性（Integrity）を維持すること」などと定義されている[5]。両者を比較した場合には、サイバーセキュリティは、紙に記された情報等、情報システムを介在させない情報を対象外[6]とする一方で、「情報システム及び情報通信ネットワークの安全性」の観点を強調し[7]、新たな技術による新たな脅威を見込んで網羅的な定義とする[8]ことで、サイバー空間に関わるリスクをより広く

---

* 本稿におけるインターネット情報の最終アクセス日は令和元年 12 月 24 日である。

1 「問 1　過去 1 年間のインターネット利用経験」総務省『平成 30 年通信利用動向調査（世帯構成員編）』2019.5.31. e-stat 政府統計の総合窓口ウェブサイト <https://www.e-stat.go.jp/stat-search/file-download?statInfId=000031831225&fileKind=1>

2 三菱総合研究所社会 ICT イノベーション本部「ICT によるイノベーションと新たなエコノミー形成に関する調査研究報告書」2018.3, p.58. 総務省ウェブサイト <http://www.soumu.go.jp/johotsusintokei/linkdata/h30_02_houkoku.pdf>

3 サイバー空間とは、「情報通信技術を用いて情報がやりとりされる、インターネットその他の仮想的な空間」（情報セキュリティ政策会議「国民を守る情報セキュリティ戦略」2010.5.11, p.16. 内閣サイバーセキュリティセンターウェブサイト <https://www.nisc.go.jp/active/kihon/pdf/senryaku.pdf>）。

4 Society5.0 とは、「サイバー空間（仮想空間）とフィジカル空間（現実空間）を高度に融合させたシステムにより、経済発展と社会的課題の解決を両立する、人間中心の社会（Society）」（「Society 5.0」内閣府ウェブサイト <https://www8.cao.go.jp/cstp/society5_0/index.html>）。サイバー空間については前掲注(3)参照。

5 “OECD Guidelines for the Security of Information Systems, 1992.” OECD website <https://www.oecd.org/internet/ieconomy/oecdguidelinesforthesecurityofinformationsystems1992.htm>

6 「法律解説［国会・内閣］サイバーセキュリティ基本法」『法令解説資料総覧』397 号, 2015.2, p.17.

7 土居範久監修「情報通信技術の進展とサイバーセキュリティ」『情報通信技術の進展とサイバーセキュリティ―科学技術に関する調査プロジェクト調査報告書―』（調査資料 2014-3）国立国会図書館調査及び立法考査局, 2015, p.1. <http://dl.ndl.go.jp/view/download/digidepo_9104276_po_20140301.pdf?contentNo=1>

8 三角育生・岡村久道「連続対談 サイバーセキュリティと法律（1）サイバーセキュリティ基本法―内閣サイバーセ

扱っていると見ることもできる。

政府は、情報セキュリティの語を用いて戦略等を策定してきたが、後述のとおり、近年では脅威の認識の変化に伴い、サイバーセキュリティの語が用いられるようになっている。ただし、両者の異同は必ずしも明らかではないとする見解もあり[9]、引き続き情報セキュリティの語が用いられている政府文書もある。

２　サイバーセキュリティ政策の経緯

（1）IT 化の進展とセキュリティ政策

日本では、平成 12 年に、閣法の「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」）が成立し、インターネット等を活用した社会を目指す動きが本格化した[10]。同法第 22 条では、「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」と規定され、情報セキュリティも施策の一部とされた。一方、平成 12 年 1 月から 2 月にかけて、政府関連機関のウェブサイトが大規模に改ざんされる事件があり[11]、これを契機として、内閣官房に情報セキュリティ対策推進室が設置されるなど省庁横断的な対策の強化が図られた[12]。

（2）情報セキュリティ政策の本格化

情報セキュリティに関わる様々なリスクが認知されるようになると、平成 15 年 7 月に策定された政府の IT 戦略である「e-Japan 戦略Ⅱ」[13]には、「安全・安心な利用環境の整備」として情報セキュリティ対策が盛り込まれた。さらに翌年の「e-Japan 戦略Ⅱ加速化パッケージ」[14]において、「セキュリティ（安全・安心）政策の強化」が重点施策とされ、情報セキュリティ補佐官が置かれた。平成 17 年、情報セキュリティ対策推進室を強化する形で、内閣官房情報セキ

キュリティセンター・三角育生審議官に聴く―」『NBL』1103 号, 2017.8.1, p.45.

9 曽我部真裕「第 6 章補論　情報セキュリティ」曽我部真裕ほか『情報法概説　第 2 版』弘文堂, 2019, p.253. また、「サイバーセキュリティ」の定義については国際的にみると、必ずしも共通の理解があるものとは言えず、近年では、外国勢力が不正確な情報の拡散などを通じて政治的な意思決定や世論等に影響を与える誘導工作（influence operation）もサイバーセキュリティ上の脅威と見る論者もいる（山下真「サイバーセキュリティの概念―国際標準化の動向を背景に―」（情報セキュリティマネジメント・セミナー2018 資料）2018.12.7. 日本ネットワークセキュリティ協会ウェブサイト <https://www.jnsa.org/seminar/2018/1207/data/2018_resume2.pdf>; 「サイバー対策　日本まず「復元力」強化　名和利男氏」『読売新聞』2019.1.17）。

10 その後の政府の IT 戦略を中心とした情報政策の展開については、以下を参照。神足祐太郎「日本における情報政策の展開―IT 基本法以降の政府 IT 戦略を中心に―」『情報通信をめぐる諸課題―科学技術に関する調査プロジェクト調査報告書―』（調査資料 2014-2）国立国会図書館調査及び立法考査局, 2015, pp.95-118. <http://dl.ndl.go.jp/view/download/digidepo_9104301_po_20140207.pdf?contentNo=1>

11 第 149 回国会参議院決算委員会会議録閉会後第 6 号　平成 12 年 9 月 20 日　p.14.

12 「情報セキュリティ対策推進室の設置に関する規則」（平成 12 年 2 月 29 日内閣総理大臣決定）内閣官房情報セキュリティ対策推進室ウェブサイト <https://www.nisc.go.jp/itso/shoukai/h160423kisoku.html>; 第 156 回国会衆議院個人情報の保護に関する特別委員会議録第 5 号　平成 15 年 4 月 17 日　p.16; 土居監修　前掲注(7), p.17.

13 IT 戦略本部「e-Japan 戦略Ⅱ」2003.7.2. 首相官邸ウェブサイト <http://www.kantei.go.jp/jp/singi/it2/kettei/030702ejapan.pdf>

14 IT 戦略本部「e-Japan 戦略 II 加速化パッケージ」2004.2.6. 同上 <https://www.kantei.go.jp/jp/singi/it2/kettei/040206ejapan.pdf>

ュリティセンター（National Information Security Center: 旧 NISC）[15]（各種略称については本稿末尾の表 2 を参照）が、さらに、同年、高度情報通信ネットワーク社会推進戦略本部（IT 戦略本部）[16]の下に、内閣官房長官を本部長とする情報セキュリティ政策会議（事務局は旧 NISC）が設置された[17]。以降、旧 NISC と、警察庁、防衛庁（平成 19 年から防衛省）、総務省、経済産業省の関係 4 省庁（平成 25 年以降は、外務省も加えた 5 省庁）を中心として、情報セキュリティ政策が推進されてきた[18]。

（3）基本法の制定

国境を越えたサイバー攻撃等による政府等の機微情報の窃取や重要インフラへの脅威への懸念が強まると、それまでの個々の主体における情報セキュリティの確保に加えて、サイバー空間の安全の確保という視点が必要であると考えられるようになっていった[19]。平成 26 年には、議員立法（衆議院内閣委員長提出）で基本法が成立した。同法では、国、地方公共団体、重要社会基盤事業者（重要インフラ事業者）、サイバー関連事業者、教育研究機関等についてサイバーセキュリティに関連した責務が定められている（第 4 条から第 11 条まで）。

政府に対しては、①サイバーセキュリティに関する施策についての基本的な方針、②国の行政機関等におけるサイバーセキュリティの確保に関する事項、③重要インフラ事業者・地方公共団体におけるサイバーセキュリティの確保の促進に関する事項を定める「サイバーセキュリティ戦略」の閣議決定による策定が義務付けられた（第 12 条）。

また、サイバーセキュリティ戦略本部（以下「本部」）を内閣に設置し、IT 戦略本部、国家安全保障会議と緊密に連携しつつ、サイバーセキュリティに関する施策を総合的かつ効果的に推進するものとされた。旧 NISC が内閣官房組織令（昭和 32 年政令第 219 号）に基づき内閣サイバーセキュリティセンター（National center of Incident readiness and Strategy for Cybersecurity: NISC）に改組され、サイバーセキュリティを推進する組織は、従来の内閣総理大臣決定等によるものから法令上の根拠を持つ組織となった。

その後、平成 28 年の改正では、日本年金機構の個人情報流出事件[20]を受けて、従前、国の行政機関に限定されていた NISC による監視、原因究明調査の対象を独立行政法人及び本部が指定する特殊法人・認可法人に広げる等の法改正が行われた[21]。さらに、平成 30 年の改正で、官

---

15 「情報セキュリティセンターの設置に関する規則」（平成 12 年 2 月 29 日内閣総理大臣決定）内閣サイバーセキュリティセンターウェブサイト <https://www.nisc.go.jp/about/pdf/050420-kisoku.pdf>

16 IT 基本法第 25 条に基づき、内閣に設置され、高度情報通信ネットワーク社会の形成に関する重点計画の作成等を行う。国務大臣、内閣情報通信政策監、有識者から構成され、本部長は内閣総理大臣である。なお、平成 25 年以降、「IT 総合戦略本部」という略称が用いられているが、本稿では「IT 戦略本部」に統一する。

17 内閣官房情報セキュリティセンター（NISC）「情報セキュリティ政策会議の設置について（IT 戦略本部決定）」2005.5.30. 内閣サイバーセキュリティセンターウェブサイト <https://www.nisc.go.jp/press/050530seisaku-press.html>

18 武智洋「第 3 章　日本のサイバーセキュリティ関連組織の現状」サイバーセキュリティと経営戦略研究会編『サイバーセキュリティ』NTT 出版, 2014, p.107.

19 「法令解説　サイバーセキュリティに関する施策を総合的かつ効果的に推進」『時の法令』1975 号, 2015.4.15, p.19; 情報セキュリティ政策会議「サイバーセキュリティ戦略―世界を率先する強靭で活力あるサイバー空間を目指して―」2013.6.10, pp.3, 5. 内閣サイバーセキュリティセンターウェブサイト <https://www.nisc.go.jp/active/kihon/pdf/cyber-security-senryaku-set.pdf> 平成 25 年のサイバーセキュリティ戦略では、平成 23 年の衆議院、参議院、防衛産業への標的型攻撃等を例示している。

20 平成 27 年、日本年金機構に対するサイバー攻撃により、約 125 万件の個人情報が流出した事件。

21 「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」（平成 28 年法律第 31 号）による改正。同時に情報処理安全確保支援士制度の創設、本部事務の一部の独立行政法人情報処理推進機構

民を含めた多様な主体が情報を迅速に共有することにより、サイバー攻撃による被害及びその拡大を防ぐことを目的としたサイバーセキュリティ協議会が創設された[22]。平成 31（令和元）年度の政府サイバーセキュリティ関係予算は約 712.9 億円である[23]（政策の経緯について本稿末尾の表 1 も参照）。

Ⅱ　政府・関係機関の施策

基本法に基づき設置された本部の下、「サイバーセキュリティ戦略」に基づき、政府及び関係機関において、サイバーセキュリティ関係の施策が実施されている。以下では、本部及び関係 5 省庁の施策を中心にその概要を紹介する[24]。

1　サイバーセキュリティ戦略本部・NISC

(1) 組織

本部は、基本法第 25 条に基づき、内閣に設置された。本部長は内閣官房長官であり、関係 5 省庁の長及び有識者から構成される（基本法第 28 条、同第 30 条）。IT 戦略本部、国家安全保障会議とも連携しつつ、サイバーセキュリティ戦略案の策定等を担っている（同第 26 条）。

NISC は、本部の事務局としての役割のほか、政府のサイバーセキュリティ政策に関する総合調整を担う。内閣官房副長官補を NISC センター長として、基本戦略、国際戦略、政府機関総合対策、情報統括、事案対処分析、東京 2020、重要インフラの 7 つのグループで構成されており、後掲の戦略の策定、政府・重要インフラのサイバーセキュリティ確保に係る業務等を担っている[25]。

(2) サイバーセキュリティ戦略

政府は、基本法第 12 条に基づき、平成 30 年に第 3 次のサイバーセキュリティ戦略[26]を閣議決定した。同戦略では、基本法の目的等[27]を踏まえ、持続的な発展のためのサイバーセキュリテ

（Information-technology Promotion Agency: IPA）への委託に係る規定の整備も行われた。

22 「サイバーセキュリティ基本法の一部を改正する法律」（平成 30 年法律第 91 号）。発足は平成 31 年 4 月（内閣サイバーセキュリティセンター（NISC）「サイバーセキュリティ基本法の一部を改正する法律の施行及び同法に基づくサイバーセキュリティ協議会の組織について」2019.4.1. <https://www.nisc.go.jp/press/pdf/kyogikai.pdf>）。

23 「政府のサイバーセキュリティに関する予算」（サイバーセキュリティ戦略本部第 21 回会合 資料 7）2019.1.24, p.1. 内閣サイバーセキュリティセンターウェブサイト <https://www.nisc.go.jp/conference/cs/dai21/pdf/21shiryou07.pdf>

24 施策・関連組織の概要については以下を参考とした。武智　前掲注(18), pp.105-150;『情報セキュリティ白書 2018』独立行政法人情報処理推進機構, 2018, pp.80-99.

25 「内閣サイバーセキュリティセンター（NISC）の組織体制」内閣サイバーセキュリティセンターウェブサイト <https://www.nisc.go.jp/about/organize.html>

26 「サイバーセキュリティ戦略」（平成 30 年 7 月 27 日閣議決定）同上 <https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku2018.pdf> 基本法制定に先立つ平成 25 年に、第 1 次のサイバーセキュリティ戦略（それ以前は「情報セキュリティ基本計画」）が情報セキュリティ政策会議決定として策定されている。

27 基本法の目的は、「経済社会の活力の向上及び持続的発展」、「国民が安全で安心して暮らせる社会の実現」、「国際社会の平和及び安全の確保並びに我が国の安全保障に寄与すること」（基本法第 1 条）である。これを踏まえ、「自由、公正かつ安全なサイバー空間」を目指すことを理念とし、施策の立案・実施にあたっては①情報の自由な流通の確保、②法の支配、③開放性、④自律性、⑤多様な主体の連携の 5 原則に従うものとされている（同上, pp.8-9）。

ィを目指し、①サービス提供者の任務保証[28]、②リスクマネジメント、③参加・連携・協働[29]の3つの観点から取組を推進するとしている。

(3) 政府機関のサイバーセキュリティ

中央省庁は、インターネットを介さずにネットワークを構成しているため(「霞ヶ関WAN」)、一部の組織の脆弱性により、政府全体がリスクにさらされることになる[30]。そこで、平成17年に、「政府機関の情報セキュリティ対策の強化に関する基本方針」[31]、「政府機関の情報セキュリティ対策のための統一基準」[32]が策定され、以降改定を重ねている。さらに、基本法第26条第1項第2号において、国の行政機関等のサイバーセキュリティに関する対策の基準を作成することとされたことを受けて、「政府機関等の情報セキュリティ対策のための統一基準群」が策定されている[33]。さらに、総務省及び経済産業省は、クラウドサービスの安全性評価に関する検討会を開催し、評価方法等を検討しており、その成果は同統一基準等の改定の際に反映される見込みである[34]。

この間には、外部からのサイバー攻撃に対し横断的監視・政府機関への助言等を行う政府機関情報セキュリティ横断監視・即応調整チーム(Government Security Operation Coordination team: GSOC)、発生事象の正確な把握、被害拡大防止等のための技術的助言等を行う情報セキュリティ緊急支援チーム(Cyber incident Mobile Assistance Team: CYMAT)の設置等、組織体制の構築も行われている[35]。

(4) 重要インフラの防護

情報通信、運輸、金融など、国民生活及び経済活動の基盤であって、その機能が停止し、又は低下した場合に国民生活又は経済活動に多大な影響を及ぼすおそれが生じるものを重要イン

---

28 政府や重要インフラ事業者等が自ら遂行すべき業務やサービス(任務)を着実に遂行するという観点。

29 不正プログラムからの防御、個人情報の適切な取扱い等の個人・組織の平時からの基本的な取組のことであり、公衆衛生活動にたとえて、サイバー衛生(Cyber Hygiene)とも呼ばれる。

30 木本裕司・佐々木良一「内閣官房情報セキュリティセンターが進める政府機関の情報セキュリティ施策」『情報の科学と技術』62(8), 2012, p.329.

31 「政府機関の情報セキュリティ対策の強化に関する基本方針」(平成17年9月15日情報セキュリティ政策会議決定)内閣サイバーセキュリティセンターウェブサイト <https://www.nisc.go.jp/active/general/pdf/2siryou04-1d.pdf>

32 「政府機関の情報セキュリティ対策のための統一基準(2005年項目限定版)」(平成17年9月15日情報セキュリティ政策会議決定)<http://dl.ndl.go.jp/view/download/digidepo_3531518_po_2siryou04-3d.pdf?contentNo=1>

33 「「政府機関等の情報セキュリティ対策のための統一基準群(平成30年度版)」について」内閣サイバーセキュリティセンターウェブサイト <https://www.nisc.go.jp/active/general/kijun30.html>

34 クラウドサービスを認証する制度を設け、基準を満たしたものを登録簿に掲載し、掲載されたサービスのみを政府機関が利用可能とするものと報じられている(「省庁向けクラウドサービス　安全確認しリスト化」『日本経済新聞』2019.3.16)。なお、クラウドサービス(コンピューティング)の定義は必ずしも一定ではないが、「共有化されたコンピュータリソース(サーバ, ストレージ, アプリケーションなど)について, 利用者の要求に応じて適宜・適切に配分し, ネットワークを通じて提供することを可能とする情報処理形態」などと定義される(経済産業省「クラウドサービス利用のための情報セキュリティマネジメントガイドライン　2013年度版」p.4. <https://www.meti.go.jp/policy/netsecurity/downloadfiles/cloudsec2013fy.pdf>)。

35 「政府機関等におけるサイバーセキュリティに関する情勢」『サイバーセキュリティ2019(2018年度報告・2019年度計画)』サイバーセキュリティ戦略本部, 2019, pp.29-30. 政府機関に対応する第一GSOCの運用開始が平成20年、独立行政法人等に対応する第二GSOCは平成29年に運用開始された。第一GSOCはNISC(情報統括グループ)、第二GSOCはIPAに置かれている。CYMATは、平成24年に設置された(各府省庁の情報セキュリティに関する技能・知見を有する職員が併任し、約40名程度)(「情報セキュリティ緊急支援チーム(CYMAT)の概要」(情報セキュリティ政策会議第30回会合 資料6-1)2012.7.4. 内閣サイバーセキュリティセンターウェブサイト <https://www.nisc.go.jp/conference/seisaku/dai30/pdf/30shiryou0601.pdf>)。

フラという[36]。政府は、平成 12 年に、「重要インフラのサイバーテロ対策に係る特別行動計画」を決定して以降、重要インフラの防護に関する計画を策定してきた[37]。

本部は、平成 29 年、「重要インフラの情報セキュリティ対策に係る第 4 次行動計画」を決定した（平成 30 年に改定）[38]。重要インフラ防護は、機能保証の考え方を踏まえ[39]、重要インフラサービスの安全かつ持続的な提供の実現を目的とする。同行動計画には、①安全基準等の整備及び浸透、②情報共有体制の強化、③障害対応体制の強化、④リスクマネジメント及び対処体制の整備、⑤防護基盤の強化の 5 つの施策が盛り込まれている。令和元年 5 月には安全基準等策定指針等が改定され、データの適切な保護や保管場所の考慮が求められた[40]。

重要インフラ事業者は、情報共有・分析のための組織として、おおむね業界ごとに 14 分野 19 のセプター（Capability for Engineering of Protection, Technical Operation, Analysis and Response: CEPTOAR）[41]を構成しており、業界団体やセキュリティ情報共有組織（Information Sharing and Analysis Center: ISAC）[42]が事務局を担っている[43]。

２　総務省

総務省は、通信・ネットワーク政策を所管しており、「IoT の安心・安全かつ適正な利用環境の構築」等の施策を実行している。平成 29 年 1 月、「IoT サイバーセキュリティアクションプログラム 2017」を公表し、Internet of Things（IoT）[44]時代に対応したサイバーセキュリティを

---

36 基本法第 3 条第 1 項における重要社会基盤事業者の定義を参照。政府の計画では、情報通信、金融、航空、空港、鉄道、電力、ガス、政府・行政サービス、医療、水道、物流、化学、クレジット、石油の 14 分野が挙げられている（「重要インフラの情報セキュリティ対策に係る第 4 次行動計画」（平成 29 年 4 月 18 日サイバーセキュリティ戦略本部決定　平成 30 年 7 月 25 日サイバーセキュリティ戦略本部改定）p.50. 同上 <https://www.nisc.go.jp/active/infra/pdf/infra_rt4_r1.pdf>）。

37 なお、基本法において、国は、重要インフラ事業者のサイバーセキュリティに関し、基準の策定、演習及び訓練、情報の共有等の施策を講じるものとされた（第 14 条）。

38 「重要インフラの情報セキュリティ対策に係る第 4 次行動計画」前掲注(36)

39 機能保証とは「各関係主体が重要インフラサービスの防護や機能維持を確約することではなく、各関係主体が重要インフラサービスの防護や機能維持のためのプロセスについて責任を持って請け合うこと」を指す（同上, pp.5-6）。

40 サイバーセキュリティ戦略本部「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針　第 5 版」（平成 30 年 4 月 4 日　令和元年 5 月 23 日改定）p.12. 内閣サイバーセキュリティセンターウェブサイト <https://www.nisc.go.jp/active/infra/pdf/shishin5rev.pdf> 同時に改定された事業者向けの手引書では「海外サーバーにおけるデータ保管・処理等」がリスクにつながり得ることが示されている（「別紙 2　結果を生じ得る事象（脅威）の例」サイバーセキュリティ戦略本部・重要インフラ専門調査会『重要インフラにおける機能保証の考え方に基づくリスクアセスメント手引書　第 1 版改定版』2019.5.23. 同 <https://www.nisc.go.jp/active/infra/files/tebikishorev.zip>; 「インフラ機密　指針改定」『読売新聞』2019.4.19; 「重要インフラ　厳格管理」『日本経済新聞』2019.4.19）。なお、中国製通信機器を通じた情報漏えい等を念頭に置いて、安全保障上のリスクがある通信機器を調達しないことも申し合わされている。

41 セプター構成員間の情報共有のほか、所管省庁（金融庁（金融）、総務省（情報通信、地方公共団体）、厚生労働省（医療、水道）、経済産業省（電力、ガス、化学、クレジット、石油）及び国土交通省（航空、空港、鉄道、物流）（「重要インフラの情報セキュリティ対策に係る第 4 次行動計画　活動内容」同上 <https://www.nisc.go.jp/active/infra/outline.html>））との間や、セプターの協議会（セプターカウンシル）を通じたセプター間の情報共有も担っている。

42 同業者間でセキュリティ情報を共有、対応力の向上につなげるための組織。日本では、平成 14 年に通信事業者の「Telecom-ISAC（現 ICT-ISAC）」が設置され、近年、金融、電力など各業界で相次いで発足している（「対サイバー　共同戦線」『読売新聞』2019.5.15, 夕刊）。

43 内閣官房内閣サイバーセキュリティセンター（NISC）「重要インフラにおけるセプターの活動状況について（2018 年度）」（重要インフラ専門調査会第 18 回会合 資料 4）2019.4.18. <https://www.nisc.go.jp/conference/cs/ciip/dai18/pdf/18shiryou04.pdf>

44 Internet of Things（IoT）は、「モノのインターネット」という意味であり、従来の情報機器間（人間間）の通信にとどまらず、自動車、工場機械等の物や人を含めたあらゆる「モノ」がインターネットにつながることを表現する

確立すべく、①「サイバーセキュリティタスクフォース」の開催、②IoT 機器セキュリティ対策の実施、③セキュリティ人材育成のスピードアップ、④総務大臣表彰制度の創設、⑤国際連携の推進の 5 つの施策を実施するとした[45]。

（1）サイバーセキュリティタスクフォース

平成 29 年 1 月、IoT/AI[46]時代のサイバーセキュリティを支える基盤・制度、人材育成等を議題とする「サイバーセキュリティタスクフォース」（座長：安田浩東京電機大学学長）が設置された。同タスクフォースは、平成 29 年 10 月に、IoT に関するセキュリティ対策の総合的な推進に向けて取り組むべき課題を「IoT セキュリティ総合対策」として公表している[47]。①脆弱性対策に係る体制の整備、②研究開発の促進、③民間企業等におけるセキュリティ対策の促進、④人材育成の強化、⑤国際連携の推進の 5 つの観点からまとめられた同総合対策は、（2）で紹介する法改正等に結び付いている[48]。同総合対策は、半年に一度検証が行われてきたが、その後の状況変化を踏まえ、令和元年 8 月、「IoT・5G セキュリティ総合対策」が策定された[49]。

（2）情報通信研究機構

国立研究開発法人情報通信研究機構（National Institute of Information and Communications Technology: NICT）には、サイバーセキュリティ研究所が置かれ、サイバー攻撃の可視化、探知等に関するシステムを開発している。また、平成 29 年 4 月には、ナショナルサイバートレーニングセンターを設置し、国・自治体・重要インフラ事業者等に向けたサイバー防衛演習を実施している[50]。加えて、第 196 回国会において成立した「電気通信事業法及び国立研究開発法人情報通信研究機構法の一部を改正する法律」（平成 30 年法律第 24 号）に基づき、インターネット上の IoT 機器に容易に推測されるパスワードを入力する手法で、設定等に不備のある機器を調査し、電気通信事業者に通知する事務を行っている[51]。この調査については、民間が行えば不正アクセスに該当しかねない行為であるという観点からの批判もある[52]。

言葉である（影島広泰編著『法律家・法務担当者のための IT 技術用語辞典』商事法務, 2017, p.76）。

45 「IoT サイバーセキュリティアクションプログラム 2017」2017.1.17. 総務省ウェブサイト <http://www.soumu.go.jp/main_content/000461785.pdf>

46 Artificial Intelligence の略であり、人工知能のことをいう。

47 サイバーセキュリティタスクフォース「IoT セキュリティ総合対策」2017.10.3. 総務省ウェブサイト <http://www.soumu.go.jp/main_content/000510701.pdf> 半年に一度を目途に検証されるものとされた。

48 サイバーセキュリティタスクフォース「IoT セキュリティ総合対策プログレスレポート 2018」2018.7, pp.13-17. 同上 <https://www.soumu.go.jp/main_content/000566458.pdf>

49 サイバーセキュリティタスクフォース「IoT・5G セキュリティ総合対策」2019.8. 同上 <https://www.soumu.go.jp/main_content/000641510.pdf>

50 「ナショナルサイバートレーニングセンター」情報通信研究機構ウェブサイト <https://nct.nict.go.jp/> なお、サイバー演習自体は平成 25 年から継続して行っている（事務局「サイバーセキュリティの現状と総務省の対応について」（サイバーセキュリティタスクフォース（第 1 回）資料 1-2）2017.1.30, p.13. 総務省ウェブサイト <http://www.soumu.go.jp/main_content/000467154.pdf>）。

51 総務省・情報通信研究機構「IoT 機器調査及び利用者への注意喚起の取組「NOTICE」の実施」2019.2.1. <https://www.nict.go.jp/press/2019/02/01-1.html> なお、同法による電気通信事業法の改正により、電気通信事業者が、サイバー攻撃に関する情報を第三者機関経由で共有することを促進する制度が設けられた（第三者機関には、後掲の通信の秘密に関する規定が適用される。）。

52 「こちら特報部　家庭や企業の IoT 機器 20 日から接続調査」『東京新聞』2019.2.2. 一方、技術的な観点や NICT の性質から、調査の妥当性を認めるものとして、武田一城「IoT 機器調査を担う NICT は諜報機関か? 実施する技術的な理由」『ZDNET Japan』2019.3.8. <https://japan.zdnet.com/article/35133765/> など。

3　経済産業省

経済産業省は、情報サービス・ソフトウェア産業の振興などを所掌しており、サイバーセキュリティ産業の振興に関する検討、各種ガイドラインの普及等を行っている[53]ほか、国家資格「情報処理安全確保支援士」制度を実施している。また、関連団体である独立行政法人情報処理推進機構（Information-technology Promotion Agency: IPA）、一般社団法人 JPCERT コーディネーションセンター（Japan Computer Emergency Response Team Coordination Center: JPCERT/CC）、技術研究組合制御システムセキュリティセンター（Control System Security Center: CSSC）でも、インシデント対応や制御システムのセキュリティに関する研究等を行っている。

（1）IPA

IPA は、「情報処理の促進に関する法律」（昭和 45 年法律第 90 号）に基づき設置された独立行政法人であり、サイバー攻撃に関する情報の収集・分析・提供等を行う IPA セキュリティセンター、サイバーセキュリティ関係の情報共有を行う「サイバー情報共有イニシアティブ（J-CSIP（ジェイシップ））」、標的型サイバー攻撃被害の低減・拡大防止のための「サイバーレスキュー隊（J-CRAT（ジェイ・クラート））」を始めとして、サイバーセキュリティに関連した各種の事業を行っている[54]。また、上述の情報処理安全確保支援士の試験事務も受託している。

（2）JPCERT/CC

JPCERT/CC は、平成 8 年に設立されたコンピュータセキュリティインシデント対応のための組織である[55]。日本国内のインシデントに関する報告の受付、対応の支援等を技術的な立場から行っており、インシデント対応に関する国際連携における日本の窓口ともなっている[56]。平成 16 年以降、経済産業省から指定を受けた法人として、IPA とともに、ソフトウェア等のセキュリティ上の欠陥に関わる情報（脆弱性関連情報）の流通業務も実施している[57]。政令で指定された法人として、サイバーセキュリティ協議会の連絡調整事務も務めている[58]。

---

53 『情報セキュリティ白書　2018』前掲注(24), pp.83-89. 例えば、産業界の直面するサイバーセキュリティ上の課題（サイバーセキュリティのビジネス化を含む。）について検討する「産業サイバーセキュリティ研究会」が平成 29 年から開催されている。

54 「セキュリティセンターについて」情報処理推進機構ウェブサイト <https://www.ipa.go.jp/security/outline/isecabst.html>

55 平成 4 年頃から、有志によるボランティア活動があったが、脅威の高まりにより組織化の必要性が指摘され、平成 8 年、日本情報処理開発協会（JIPDEC。現在の「日本情報経済社会推進協会」）の一部署として設置。平成 15 年に独立（「会員 （チーム） 情報　JPCERT/CC」日本シーサート協議会ウェブサイト <https://www.nca.gr.jp/member/jpcertcc.html>; 歌代和正「JPCERT/CC 立ち上げのころの話」2009.6.19. JPCERT/CC ウェブサイト <https://www.jpcert.or.jp/magazine/10th/beginning.html>）。

56 武智　前掲注(18), pp.120-121.

57 「ソフトウエア等脆弱性関連情報取扱基準」（平成 16 年経済産業省告示第 235 号）及び「受付機関及び調整機関を定める告示」（平成 16 年経済産業省告示第 236 号）<https://www.meti.go.jp/policy/netsecurity/downloadfiles/vulhandlingG.pdf>;「脆弱性情報ハンドリングとは?」2019.5.30. JPCERT/CC ウェブサイト <https://www.jpcert.or.jp/vh/> 現在の根拠規定は次の両告示である。「ソフトウエア製品等の脆弱性関連情報に関する取扱規程」（平成 29 年経済産業省告示第 19 号）<http://www.meti.go.jp/policy/netsecurity/vul_notification.pdf> 及び「受付機関及び調整機関を定める告示」（平成 31 年経済産業省告示第 19 号）<http://www.meti.go.jp/policy/netsecurity/vul_institutions.pdf>

58 サイバーセキュリティ基本法施行令（平成 26 年政令第 400 号）第 5 条。内閣官房内閣サイバーセキュリティセンター基本戦略第 2 グループ「サイバーセキュリティ協議会について」2019.8. <https://www.nisc.go.jp/conference/cs/kyogikai/pdf/kyogikai_gaiyou.pdf>

（3）CSSC

CSSC は、平成 24 年、「技術研究組合法」（昭和 36 年法律第 81 号）に基づく経済産業大臣認可法人として設立された[59]。CSSC では、重要インフラの制御システムのセキュリティ確保を目的として、研究開発、評価認証等の活動を行っている[60]。サイバーセキュリティ演習、研究開発への活用のため、9 種の模擬プラントを設置したテストベッド施設[61]も運用している[62]。

4　警察

（1）組織

国家公安委員会の下に置かれる警察庁は、警察に関する政策立案・企画を行うとともに国の公安及び広域犯罪等を担当しており、各都道府県警は同庁と連携しながら、サイバー犯罪[63]への対応を行っている。また、サイバー攻撃への対策として、警察庁ではサイバー攻撃対策室が各都道府県警における捜査の指導・調整等に当たるとともに、同室長を長とするサイバー攻撃分析センターにおいてサイバー攻撃に係る情報の集約・分析を行っている[64]。

関連団体として、平成 26 年 11 月、産学官の情報共有・連携等を目的とした一般財団法人日本サイバー犯罪対策センター（Japan Cybercrime Control Center: JC3）が設置されており[65]、金融犯罪等サイバー空間における脅威情報の共有等を行っている。また、平成 18 年から警察庁の委託を受けて民間団体が運営するインターネット・ホットラインセンターでは、違法情報の通報を受け付け、一定の基準に基づいて選別した上で、警察へ通報、インターネットサービスプロバイダ（ISP）への削除依頼等を行っている[66]。

（2）警察におけるサイバーセキュリティ戦略

警察庁次長依命通達として「警察におけるサイバーセキュリティ戦略」[67]が発出され、これに

---

59 「当センターの概要」2019.4.1. CSSC ウェブサイト <http://www.css-center.or.jp/ja/aboutus/index.html>

60 「3.1　制御システム」『情報通信技術の進展とサイバーセキュリティ―科学技術に関する調査プロジェクト調査報告書―』前掲注(7), p.135. <http://dl.ndl.go.jp/view/download/digidepo_9104286_po_20140311.pdf?contentNo=1>

61 実際にシステムが運用される環境に近い状況で試験を行うための試験用環境のことをいう。

62 「テストベッド施設」CSSC ウェブサイト <http://www.css-center.or.jp/ja/research/css-base6.html>

63 サイバー犯罪とは、「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又は電磁的記録を対象とした犯罪等の情報技術を利用した犯罪」（「第 3 節　新たな課題への対応と今後の展望」『警察白書　平成 30 年版』警察庁ウェブサイト <https://www.npa.go.jp/hakusyo/h30/honbun/html/uf130000.html>）。電磁的記録の定義等の追加等を行った昭和 62 年の刑法改正以降、情報化に伴う新たな犯罪類型への対応、サイバー犯罪捜査のための規定の整備のため、刑法（明治 40 年法律第 45 号）、刑事訴訟法（昭和 23 年法律第 131 号）の改正等が行われている。経緯については以下を参照。石井夏生利「第 9 章　情報セキュリティ」岡村久道編著『インターネットの法律問題』新日本法規出版, 2013, pp.278-316; 岡村久道・安冨潔「連続対談 サイバーセキュリティと法律（3）サイバーセキュリティと刑事法」『NBL』1106 号, 2017.9.15, pp.47-57.

64 「3　サイバー攻撃への対策」『警察白書　令和元年版』同上 <https://www.npa.go.jp/hakusyo/r01/honbun/html/v3323000.html> 政府機関、重要インフラ事業者等が多く所在する 14 都道府県警においてはサイバー攻撃特別捜査隊も設置されている。

65 「一般財団法人日本サイバー犯罪対策センター 設立趣意」日本サイバー犯罪対策センターウェブサイト <https://www.jc3.or.jp/about/concept.html>

66 「ホットラインセンターについて」インターネット・ホットラインセンターウェブサイト <http://www.internethotline.jp/pages/about/index> 平成 28 年 4 月から一般社団法人セーファーインターネット協会が受託（「【プレスリリース】SIA、インターネット上の違法・有害情報対策の 2016 年実績を公開」2017.6.6. セーファーインターネット協会ウェブサイト <https://www.saferinternet.or.jp/info/1061/>）。

67 警察庁次長「警察におけるサイバーセキュリティ戦略の改定について（依命通達）」2018.9.6. <https://www.npa.go.jp/cybersecurity/pdf/300906_senryaku.pdf>

基づき各種の対応が採られている。同戦略は、①サイバー空間の脅威への対応の強化、②警察における組織基盤の更なる強化、③国際連携及び産学官連携の推進を3つの柱としている。サイバー犯罪に対する捜査等の推進、国の公安を脅かす事案の防止及び対処等のほか、産学官の知見を活用した対策の推進として、JC3 等との連携を通じ、産学官の情報や知見をサイバー犯罪・サイバー攻撃の取締り及び被害防止対策に活用するものとされている。

（3）サイバー犯罪の動向

平成30年中のサイバー犯罪検挙件数は、9,040件で、過去最多となっている[68]。一方、単なるいたずらのようなプログラムや新たに生まれた技術を、不正指令電磁的記録に関する罪[69]（刑法（明治40年法律第45号）第19章の2）として摘発する例が相次いだため、警察の取締りの在り方には懸念も生じている[70]。同罪が適用されるか否かの基準が曖昧で、これまで考えられてきたよりも広範に適用されたことから、IT業界の萎縮を招きかねないという批判もあった[71]。

５　防衛省

サイバー攻撃は、安全保障上の課題としても認識されるようになっており、日本でも平成23年の「平成23年度以降に係る防衛計画の大綱」において、サイバー攻撃のための対処態勢等が取り上げられた[72]。平成26年3月には、自衛隊統合幕僚監部自衛隊指揮通信システム隊の下に、防衛省・自衛隊のネットワーク防護を任務とする「サイバー防衛隊」（令和元年度人員は 220名[73]）が設置されており、①24時間体制でのネットワーク監視、事案対処、②サイバー攻撃に関する情報収集等を行っている[74]。このほか、現状では、陸海空の自衛隊にそれぞれサイバー防

---

68 警察庁「平成30年におけるサイバー空間をめぐる脅威の情勢等について」2019.3.7. <http://www.npa.go.jp/publications/statistics/cybersecurity/data/H30_cyber_jousei.pdf> これは前年から26件増加して過去最多である（「第3章　サイバー空間の安全の確保」『警察白書　令和元年版』前掲注(64) <https://www.npa.go.jp/hakusyo/r01/honbun/html/v3310000.html>）。件数には、「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）違反、不正指令電磁的記録に関する罪（刑法第19章の2）、コンピュータ・電磁的記録対象犯罪（電子計算機使用詐欺等）、その他（ネットワークを利用した著作権法（昭和45年法律第48号）違反等）を含む。

69 「人が電子計算機を使用するに際してその意図に沿うべき動作をさせず、又はその意図に反する動作をさせるべき不正な指令を与える電磁的記録」の作成・供用等に関する罪（刑法第168条の2）及びその取得・保管に関する罪（同第168条の3）。いわゆるコンピュータウイルスなどが想定される（石井　前掲注(63), p.293）。

70 出口絢「コインハイブ事件、経緯総まとめ　「ウイルス罪」相次ぐ摘発に萎縮も」『弁護士ドットコムニュース』2019.3.26. <https://www.bengo4.com/c_23/n_9421/>

71 同上; 杉浦隆幸「論点　ウイルス「不正」基準明確化を」『読売新聞』2019.5.30; 村上万純「「いたずらURL貼って補導」がIT業界の萎縮をまねく理由」『IT media News』, 2019.3.8. <https://www.itmedia.co.jp/news/articles/1903/08/news119.html> なお、同罪が追加された平成23年改正時の審議に当たっては、「不正指令電磁的記録であることを認識認容しつつ実行する目的であることなど同罪の構成要件の意義を周知徹底することに努めること」や「その捜査等に当たっては、憲法の保障する表現の自由を踏まえ、ソフトウエアの開発や流通等に対して影響が生じることのないよう、適切な運用に努めること」を含む、参議院法務委員会附帯決議が行われている（第177回国会参議院法務委員会会議録第17号　平成23年6月16日　p.14）。ウェブサイト閲覧時に仮想通貨を獲得するための演算を行わせるプログラムを埋め込んだことが不正指令電磁的記録保管の罪（刑法第168条の3）に問われた事件について、横浜地方裁判所は無罪判決を下している（「社説　ネット犯罪摘発　行きすぎ戒める判決だ」『朝日新聞』2019.3.30）。

72 「平成23年度以降に係る防衛計画の大綱について」（平成22年12月17日安全保障会議決定・閣議決定）防衛省・自衛隊ウェブサイト <https://www.mod.go.jp/j/approach/agenda/guideline/2011/taikou.pdf>

73 第200回国会参議院外交防衛委員会会議録第2号　令和元年11月7日　p.20.

74 「5.3.2　サイバー空間における安全保障」『情報通信技術の進展とサイバーセキュリティ―科学技術に関する調査プロジェクト調査報告書―』前掲注(7), p.185. <http://dl.ndl.go.jp/view/download/digidepo_9104288_po_20140313.pdf?contentNo=1>

衛の専門部隊が存在するが、今後、共同の部隊[75]として「サイバー防衛部隊」を新編し、全体の規模を千数百名規模まで拡充する計画である[76]。こうした専門組織による対応のほか、米国を含む関係機関・各国との連携がサイバー防衛の柱とされており、平成 31 年 4 月の外務・防衛担当閣僚協議では、サイバー攻撃も日米安全保障条約の対象とされることが確認された[77]。

また、防衛省では安全保障を揺るがすようなサイバー攻撃を受けた場合に反撃するためのコンピュータウイルスを作成・保有する方針を固めたと報じられている[78]。

６　外務省

外務省は、「サイバーセキュリティ戦略」において、「国際社会の平和・安定及び我が国の安全保障への寄与」のうち、「自由、公正かつ安全なサイバー空間の理念の発信」、「国際協力・連携」等を担当するものとされており、サイバー空間における法の支配の推進、信頼醸成措置の推進、能力構築支援等の取組等の「サイバー外交」の取組を進めている[79]。

Ⅲ　サイバーセキュリティ政策の評価と課題

１　日本のサイバーセキュリティに対する評価と組織体制

国際電気通信連合（International Telecommunication Union: ITU）が、各国のサイバーセキュリティについて評価する Global Cybersecurity Index（GCI）で、日本は、高いレベルの対応を行っている国に分類され、175 か国中世界 14 位にランキングされている[80]。このように、日本のサイバーセキュリティの現状は、一定の評価を受けている[81]。

その一方で指摘されている課題として、施策の実施に当たっての組織体制の問題がある。例えば、基本法改正により協議会が設置された後も、現存する多様な組織が統廃合されず、情報の一元化が困難であるともいわれる[82]。また、諸外国に存在するような国全体のサイバーセキ

---

75 陸上自衛隊、海上自衛隊又は航空自衛隊の防衛大臣直轄部隊で、統合運用による円滑な任務遂行上一体的運営を図る必要がある場合に置かれる、陸上自衛隊、海上自衛隊及び航空自衛隊の共同の部隊をいう（自衛隊法（昭和 29 年法律第 165 号）第 21 条の 2）。

76 「平成 31 年度以降に係る防衛計画の大綱について」（平成 30 年 12 月 18 日国家安全保障会議決定・閣議決定）pp.24, 30. 防衛省・自衛隊ウェブサイト <https://www.mod.go.jp/j/approach/agenda/guideline/2019/pdf/20181218.pdf>; 「＜解説＞サイバー防衛部隊の新編」『防衛白書　令和元年度』同 <https://www.mod.go.jp/j/publication/wp/wp2019/html/nc011000.html>; 第 198 回国会衆議院会議録第 24 号　令和元年 5 月 16 日　p.13.

77 「日米安全保障協議委員会共同発表（仮訳）」2019.4.19. 外務省ウェブサイト <https://www.mofa.go.jp/mofaj/files/000470737.pdf> サイバー攻撃についても、「物理的手段による攻撃と同様の極めて深刻な被害が発生し、これが相手方により組織的、計画的に行われている場合には武力攻撃に当たり得る」として、自衛権行使が可能な場合があると答弁している（第 198 回国会衆議院会議録第 24 号　令和元年 5 月 16 日　p.13.　安倍晋三首相答弁）。

78 「サイバー反撃ウイルス保有へ」『東京新聞』2019.4.30.

79 「サイバーセキュリティ　日本のサイバー外交」2019.11.20. 外務省ウェブサイト <https://www.mofa.go.jp/mofaj/annai/page5_000250.html>

80 *Global Cybersecurity Index (GCI) 2018*, International Telecommunication Union, 2019, p.58. <https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf> 評価は、法的対応、技術的対応、組織体制、能力向上、国際連携の観点から行われている。

81 例えば、サーレライネン（Matti Saarelainen）EU・NATO ハイブリッド脅威対策センター（European Centre of Excellence for Countering Hybrid Threats）所長は、「日本はすでに様々な対策を練っており、技術的にも能力の高い人が多い」として、攻撃が難しいと評価している（飯塚恵子『ドキュメント誘導工作―情報操作の巧妙な罠―』中央公論新社, 2019, p.286）。

82 名和利男サイバーディフェンス研究所上席分析官による。同上, p.250.

ュリティに関わる実務を行う一元化された実務組織が存在していないこと、各省庁がサイバーセキュリティ施策を実施しているものの省庁縦割りの限界があることが指摘されている[83]。そこで、政府がより主導的な役割を果たすための一元化された実務機関として、内閣府外局としてサイバーセキュリティ庁を設置するべきだとの提言もある[84]。

２　通信の秘密をめぐる議論

サイバー攻撃への対策を実施する場合には、攻撃者の探知や特定の通信の遮断など、通信に係る情報を取得することが必要となる場合がある。一方で、日本国憲法第 21 条第 2 項は「通信の秘密は、これを侵してはならない」と規定し、「電気通信事業法」（昭和 59 年法律第 86 号）でも、罰則をもって、通信の秘密の保護を規定している（第 4 条、第 179 条）。通信の秘密には、通信内容のほか、通信の日時、場所、当事者の氏名、通信回数などの事項（メタ情報）も含まれると解されている[85]。サイバー攻撃への対策に必要な通信に係る情報の取得が、通信の秘密の侵害に当たらないためには、通信当事者の同意又は正当防衛、緊急避難などの違法性阻却事由が必要とされる。こうした通信の秘密の保護の在り方は諸外国と比較しても厳格で[86]、サイバー攻撃を事前に探知したり、攻撃者を特定したりするための、ネットの監視体制が整っていないという指摘がある[87]。他方、通信の秘密は、「表現と人権が守られ、誰もが安全に安心して利用できる」というインターネットの自由の基盤となってきた側面もあるとされ、仮に通信の秘密に当たる情報の共有・分析等を行う場合には、その濫用を防ぎプライバシーを確保するための組織的・手続的保証が必要であり、場合によっては独立性の高い監視機関の設置も必要となるという論者もいる[88]。

---

83 例えば、英国では、2016 年、複数の省庁にまたがっていた関連組織を統合して、政府通信本部（Government Communications Headquarters: GCHQ）に、実働組織としての国家サイバーセキュリティセンター（National Cyber Security Centre: NCSC）が設置されている。NCSC は、サイバー攻撃に関する統一的な連絡窓口であり、攻撃への対応のほか、指針の作成等を行っている（“About the NCSC.” National Cyber Security Centre website <https://www.ncsc.gov.uk/section/about-ncsc/what-we-do>; 公益財団法人笹川平和財団安全保障事業グループ「サイバー空間の防衛力強化プロジェクト政策提言　“日本にサイバーセキュリティ庁の創設を！”」2018.10, pp.7-9. <https://www.spf.org/global-data/cyber_security_2018_web.pdf>）。また、攻撃対象となるインフラによっても、対応する省庁が縦割りとなっており、情報収集が難しいことも指摘されている（ロバート・ビッグマンほか「東京五輪「サイバー攻撃」が始まった」『文藝春秋』97(7), 2019.7, p.193）。

84 公益財団法人笹川平和財団安全保障事業グループ　同上, p.29.

85 多賀谷一照ほか『電気通信事業法逐条解説』電気通信振興会, 2008, p.38.

86 情報セキュリティ大学院大学「インターネットと通信の秘密」研究会「「インターネットと通信の秘密」第 2 期研究会報告書　インターネット時代の「通信の秘密」各国比較」2014.5, p.i. キヤノングローバル戦略研究所ウェブサイト <https://www.canon-igs.org/research_papers/pdf/201405_sog_report.pdf>

87 「特集　世界デジタルサミット 2018　サイバー攻撃切り抜けろ　サイバー・ウォーフェアと世界協調」『日本経済新聞』2018.6.25; 土屋大洋「アトリビューションと抑止がカギ　日本の法律では対抗できない」『ニューリーダー』31(2), 2018.2, pp.22-25. 範囲（通信内容かメタ情報か、リアルタイムかログ情報かを含む。）、手続を含めた通信傍受に関する議論を行う必要性を指摘するものとして以下を参照。林紘一郎「サイバーセキュリティと通信の秘密」土屋大洋監修『仮想戦争の終わり―サイバー戦争とセキュリティ―』（角川インターネット講座　13）KADOKAWA, 2014, pp.206-209.

88 「（耕論）サイト遮断と言うけど　赤松健さん　宍戸常寿さん　別所直哉さん」『朝日新聞』2018.9.7. 諸外国においてインターネットの自由の基盤となっている、表現の自由やプライバシー保護が、日本ではそれほどには強くないことが指摘される。その中で、通信の秘密の保護は諸外国からも評価されてきた面があるという（宍戸常寿「現実空間と同じようにサイバー空間を守るために必要なこと　問題は「海賊版サイト」だけじゃない」『Wedge Infinity』2018.12.26. <http://wedge.ismedia.jp/articles/-/14830>）。

３　人材育成

NISC、NICT、IPA を始めとした各機関による、演習、育成プログラムの実施及び提供、国家資格によるスキルの可視化等、サイバーセキュリティ人材の育成・確保に関する施策が行われる一方[89]、セキュリティ人材は、平成 30 年時点で約 16 万人、令和 2 年時点で約 19 万人が不足するとの推計がある[90]。絶対数の不足に加え、実務に耐える高度人材の不足や地域的な偏在が指摘されている[91]。ただし、上記のような推計は、あるべき姿を描いたもので、企業側の実感とはかい離があるとも報じられている[92]。ニーズに基づくより具体的な人材像、スキルの把握、これに沿った人材の育成が必要であるという見解[93]のほか、経営者層の認識を改める必要に言及するものもある[94]。

おわりに

情報通信ネットワークや情報システムは、今や、社会全体に浸透し、その安全、信頼性の確保の重要性に議論の余地はない。例えば、平成 27 年に発生した日本年金機構からの大規模な個人情報の流出については、適切な対応が採られなかったこともあって厳しい批判を浴びた[95]。また、国外では、放送局、金融機関、電力などのインフラがサイバー攻撃によって機能停止に陥った例もある。他方、サイバーセキュリティのリスクは誇大に主張されていると指摘されることもある[96]。セキュリティ確保のためのシステムを構築したものの、結果的に使われないままに終わってしまった例もあること[97]を考えれば、セキュリティのリスクを正確に評価し、効果的な対策を検討することが望まれる。

---

89 谷脇康彦『サイバーセキュリティ』岩波書店, 2018, pp.84-96. ほかにも、文部科学省が展開する ICT 人材の育成プログラムである enPiT（Education Network for Practical Information Technologies）でも大学間や関係機関、産業界が連携した実践的な教育がなされているという（「Basic SecCap」enPiT Security ウェブサイト <http://www.seccap.jp/basic/seccap.html>）。

90 商務情報政策局情報処理振興課「IT 人材の最新動向と将来推計に関する調査結果―報告書概要版―」2016.6.10, p.12. 経済産業省ウェブサイト <https://www.meti.go.jp/policy/it_policy/jinzai/27FY/ITjinzai_report_summary.pdf>

91 名和利男「サイバー攻撃が交通網を襲う」『文藝春秋』94(10), 2016.7, p.271; 上原哲太郎「第 359 号コラム「情報セキュリティ人材が足りない、は本当か」」2015.4.27. デジタル・フォレンジック研究会ウェブサイト <https://digitalforensic.jp/2015/04/27/column359/>;「「サイバーセキュリティ人材育成分科会」第 1 次取りまとめ」2019.6. 総務省ウェブサイト <http://www.soumu.go.jp/main_content/000626983.pdf>

92 「サイバー人材不足　温度差なぜ　経産省「攻撃対策あと 19 万人」　企業は「切迫感ない」　稼がぬ部門　外注任せ」『日経産業新聞』2018.8.27. 名和　同上でも、サイバーセキュリティ担当者は直接に売上げに貢献せず、リストラの対象となってしまうことが指摘されている。

93 上原　前掲注(91); 中山貴禎「「情報セキュリティ人材が足りない」は本当か」『ZDNet Japan』2016.2.11. <https://japan.zdnet.com/article/35077012/>

94 武田一城「セキュリティ人材の末路　人数不足と育成の必要性は本当なのか?」『ZDNet Japan』2018.2.26. <https://japan.zdnet.com/article/35114853/4/>

95 「社説　年金機構と厚労省は責任感と緊張感を」『日本経済新聞』2015.8.25.

96 「IPA サイバーセキュリティシンポジウム 2014「2012 年ロンドンオリンピックのセキュリティ～我々の経験をご紹介～」オリバー・ホーア氏講演録」情報処理推進機構, 2014.2.19, p.8. <https://www.ipa.go.jp/files/000039004.pdf>

97 「政府共通プラットフォームにおけるセキュアゾーンの整備について」2019.10.28. 会計検査院ウェブサイト <https://www.jbaudit.go.jp/pr/kensa/result/31/pdf/11028_zenbun_01.pdf>

表１　国内外の政府機関・重要インフラに対する主なサイバー攻撃と政策

2000	・中央省庁ウェブサイト改ざん事件。これを受け、内閣官房に情報セキュリティ対策推進室設置 ・IT 基本法成立 ・「重要インフラのサイバーテロ対策に係る特別行動計画」を決定
2003	・「e-Japan 戦略Ⅱ」に情報セキュリティ対策が盛り込まれる。
2005	・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設置 ・「政府機関の情報セキュリティ対策の強化に関する基本方針」策定
2007	・政府、銀行などに対する大規模な DDoS 攻撃 (注1)（エストニア）
2010	・Stuxnet による核開発施設への攻撃。原発でも被害（イラン等）
2011	・三菱重工業等大手重機メーカーへのサイバー攻撃 ・衆議院・参議院への標的型攻撃
2013	・放送局や金融機関などが同時多発的にサイバー攻撃を受け社内システムが使用できなくなった（韓国）
2014	・「サイバーセキュリティ基本法」（以下「基本法」）成立 ・製鉄所のシステムが破壊されたことが発覚（ドイツ）
2015	・基本法下で初めての「サイバーセキュリティ戦略」を閣議決定 ・日本年金機構への攻撃で個人情報が流出 ・基本法施行に伴い、サイバーセキュリティ戦略本部設置、NISC 改組 ・サイバー攻撃による大規模停電（ウクライナ） ・民主党全国委員会のシステムがロシアのハッキングを受け、陣営のメールが流出（米国） ・テレビネットワークへの攻撃で 11 局が放送中断（フランス）
2016	・「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」（平成 28 年法律第 31 号）による基本法改正 ・キエフ市内で電力供給先の 5 分の 1 が約 1 時間停電（ウクライナ） ・空港システムに対する不正アクセスで搭乗手続の遅れ等が発生（ベトナム）
2017	・ランサムウェア（WannaCry）(注2) 流行により、一部医療機関等に影響（国際）
2018	・新しい「サイバーセキュリティ戦略」を閣議決定 ・サイバーセキュリティ基本法改正でサイバーセキュリティ協議会を設置

（注 1）サービス妨害（Denial of Service: DoS）攻撃は、標的となるマシンの通信量等を増加させるなどの方法でネットワークを利用不可能にすること等を意図した攻撃。ネットワーク上の多数のマシンから行うものを分散型サービス妨害（Distributed Denial of Service: DDoS）攻撃という。
（注 2）コンピュータ内のファイルを暗号化し、暗号化を解除する見返りとして身代金を要求する不正なプログラム。
（出典）「情報通信技術の進展とサイバーセキュリティに関する年表」『情報通信技術の進展とサイバーセキュリティ―科学技術に関する調査プロジェクト調査報告書―』（調査資料 2014-3）国立国会図書館調査及び立法考査局, 2015, pp.239-246. <http://dl.ndl.go.jp/view/download/digidepo_9104292_po_20140317.pdf?contentNo=1>; 各年の『情報セキュリティ白書』情報処理推進機構等に基づき筆者作成。

表２　主な略語一覧

CEPTOAR	Capability for Engineering of Protection, Technical Operation, Analysis and Response　重要インフラ事業者等の情報共有・分析機能及びこれを担う組織
CSSC	技術研究組合制御システムセキュリティセンター（Control System Security Center）
CYMAT	情報セキュリティ緊急支援チーム（Cyber incident Mobile Assistance Team）
GSOC	政府機関情報セキュリティ横断監視・即応調整チーム（Government Security Operation Coordination team）
IPA	独立行政法人情報処理推進機構（Information-technology Promotion Agency）
ISAC	セキュリティ情報共有組織（Information Sharing and Analysis Center）
JC3	一般財団法人日本サイバー犯罪対策センター（Japan Cybercrime Control Center）
JPCERT/CC	一般社団法人 JPCERT コーディネーションセンター（Japan Computer Emergency Response Team Coordination Center）
NICT	国立研究開発法人情報通信研究機構（National Institute of Information and Communications Technology）
NISC	内閣サイバーセキュリティセンター（National center of Incident readiness and Strategy for Cybersecurity）
旧 NISC	内閣官房情報セキュリティセンター（National Information Security Center）

（出典）各種資料に基づき筆者作成。