Ⅱ-5
サイバーセキュリティに関する法律及び制度

5.1　政策・制度

5.1.1　日本の情報セキュリティ政策

日本政府における情報セキュリティ政策は、情報セキュリティ政策の基本戦略を決定する「サイバーセキュリティ戦略本部」と、基本戦略の立案並びにその他官民における統一的、横断的な情報セキュリティ対策の推進に係る企画立案及び総合調整を行う「内閣サイバーセキュリティセンター（NISC）」が中心となって推進している。

日本政府における情報セキュリティ政策の最高決定機関は、「サイバーセキュリティ基本法」（平成26年法律第104号）に基づき、内閣に設置された情報セキュリティ政策の基本戦略を決定する「サイバーセキュリティ戦略本部」である。サイバーセキュリティ戦略本部は内閣官房長官を本部長、情報通信技術（IT）政策担当大臣を副本部長とし、国家公安委員会委員長、防衛大臣、総務大臣、外務大臣、経済産業大臣及び内閣総理大臣が任命する有識者で主に構成される。サイバーセキュリティ戦略本部が業務を引き継いだ情報セキュリティ政策会議はサイバーセキュリティ政策に係る中長期の計画である「サイバーセキュリティ戦略」等を策定するとともに、年次計画や年次報告を作成してきた。

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））は、情報セキュリティ政策会議、サイバーセキュリティ戦略本部の事務局として、情報セキュリティ庶務協力5省庁（警察庁、防衛省、総務省、外務省、経済産業省）の協力も得て、①情報セキュリティ政策に関する中長期計画や年度計画の立案、②情報セキュリティ政策に関する国際連携の窓口機能、③政府機関の情報セキュリティ対策を推進するための統一的な基準の策定と運用、④サイバー攻撃等に関する情報の収集・集約及び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）の運用、⑤重要インフラ行動計画に基づく情報セキュリティ対策の官民連携、⑥サイバー攻撃事案の対処調整、不正プログラムの分析等を推進してきた。なお、サイバーセキュリティ基本法の施行に伴い、NISCは、内閣総理大臣決定から政令に基づく組織となっている。NISCの下で、情報セキュリティ庶務協力5省庁をはじめとする各府省が所掌事務の中で情報セキュリティ政策・対策を推進している。

警察庁では、長官官房審議官（サイバーセキュリティ担当）の下、生活安全局がサイバー犯罪対策（情報技術犯罪対策課）、警備局がサイバー攻撃対策（サイバー攻撃分析センター）、情報通信局が技術支援（サイバーテロ対策技術室、高度情報技術解析センター）等を行っている。

防衛省は副大臣を長とするサイバー政策検討委員会を設置するとともに、2014年防衛省・自衛隊のネットワークの監視及びサイバー攻撃への対策を行うサイバー防衛隊を自衛隊に設置した。

総務省は、通信事業者（Telecom-ISAC Japan）と情報共有を図りつつ、官公庁や大企業等を対象とした実践的サイバー防御演習（CYDER）、一般利用者向けマルウェア配布サイト対策（ACTIVEプロジェクト）、情報通信研究機構（NICT）における研究開発等に取り組んでいる。

経済産業省は、情報処理推進機構（IPA）やJPCERTコーディネーションセンター（JPCERT/CC）を通じてソフトウェアや情報システムにおける情報セキュリティ対策を進めるとともに、情報セキュリティ監査制度の推進、重要インフラの制御システムの情報セキュリティに関する研究開発等を行う制御システムセキュリティセンター（CSSC）の支援等を行っている。また、

総務省と経済産業省は、サイバー攻撃対処の官民連携を図るために関連4団体と「サイバー攻撃解析協議会」を設置している。

●事例研究

■サイバーセキュリティ戦略

2013年6月10日に情報セキュリティ政策会議が決定した「サイバーセキュリティ戦略」では、基本的な考え方として、①情報の自由な流通の確保、②深刻化するリスクへの新たな対応、③リスクベースによる対応の強化、④社会的責務を踏まえた行動と共助の4つを掲げている。その上で2015年度までの3年間で、①「強靭な」サイバー空間の構築、②「活力ある」サイバー空間の構築、③「世界を率先する」サイバー空間の構築の3つを目標として掲げている。(1)

■サイバーセキュリティ国際連携取組方針

2013年10月2日に情報セキュリティ政策会議が決定した「サイバーセキュリティ国際連携取組方針」は、サイバーセキュリティ分野における国際連携・共助に関する基本方針及び重点取組分野等を整理したものである。基本原則はサイバーセキュリティ戦略を踏襲しているが、方針として①グローバルな共通認識の漸進的な醸成、②グローバルコミュニティへの我が国の貢献、③技術フロンティアのグローバルな拡大を掲げ、重点取組分野として①サイバー事案への動的対応の実践、②動的対応に備えた「基礎体力」の向上、③サイバーセキュリティに関する国際的なルール作りを推進するとしている。(2)

■政府機関の情報セキュリティ対策のための統一基準群

NISCでは政府機関の情報セキュリティ対策の水準底上げのため、統一規範、指針、統一基準、ガイドライン、マニュアルからなる政府機関統一基準群を整備している。

●海外の状況、技術動向、制度、規制

■米国のサイバーセキュリティ政策

米国のサイバーセキュリティ政策は、国家安全保障上の重要な課題として位置づけられている。2010年に発表された「国家安全保障戦略（National Security Strategy）」においても、安全保障上の最優先課題の一つにサイバーセキュリティの確保を挙げ、先端的な研究開発や人材育成を促進し、政府内をはじめ、民間セクターや諸外国等との連携を進めるとしている(3)。

■EUのサイバーセキュリティ政策

EUのサイバーセキュリティ政策は、オープンで自由なサイバー空間を維持するため、サイバー空間においても基本的人権、民主主義が守られること等を基本原則として掲げ、優先対応項目として、①サイバーレジリエンスの向上、②サイバー犯罪の激減、③共通安全保障・防衛政策に関するサイバー防衛政策・能力の確立、④サイバーセキュリティの産業・技術資源の確保、⑤首尾一貫した国際戦略の確立を通じたEUの核心的な価値の促進の5つを掲げている(4)。

(1)　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. <http://www.nisc.go.jp/active/kihon/pdf/cyber-security-senryaku-set.pdf>
(2)　情報セキュリティ政策会議「サイバーセキュリティ国際連携取組方針―j-initiative for Cybersecurity―」2013.10.2, pp.2-9. <http://www.nisc.go.jp/active/kihon/pdf/InternationalStrategyonCybersecurityCooperation_j.pdf>
(3)　The White House,“National Security Strategy,”May 2010, pp.27-28. <http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf>
(4)　European Commission and High Representative of the European Union for Foreign Affairs and Security Policy,“Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (JOIN(2013)1 final),”February 7, 2013, pp.4-5. <http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf>

5.1.2　政府機関の情報セキュリティ対策

日本政府における情報セキュリティ対策は、情報セキュリティ政策会議が策定する政府統一基準に従い各府省庁によって実施・運用されている。政府機関の横断的な組織として、政府機関監視・即応調整チーム（GSOC）や情報セキュリティ緊急支援チーム（CYMAT）が設置されている。

（1）　政府機関における情報セキュリティ体制の整備

日本の情報セキュリティ対策は、長く府省庁ごとに運用がなされてきた。しかし、2000年1月の府省庁ホームページ改ざん事件を受けて内閣官房情報セキュリティ対策推進室が同年2月に設置され、情報セキュリティポリシーに関するガイドライン策定等を行った。その後、2005年4月には対策推進室を発展させた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））、同年5月には日本の情報セキュリティ政策に関する基本戦略を決定する組織として、情報セキュリティ政策会議が高度情報通信ネットワーク社会推進戦略本部に設置された（事務局はNISCが務める。）[(1)]。2005年9月には情報セキュリティ政策会議において、①府省庁間における情報セキュリティ対策の水準の格差、②進化するIT環境に対応した適切な情報セキュリティ対策を実施できる人材の不足、③政府機関に対するDoS攻撃及び民間企業における情報漏えい事件の発生等を踏まえて、政府機関統一基準の策定や各府省庁での情報セキュリティポリシー等の見直し等を定めた「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」が決定され、これに基づき情報セキュリティ対策の整合化・共通化を促進するため「政府機関の情報セキュリティ対策における統一基準の策定と運用等に関する指針」が定められた[(2)]。同年12月には「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12月版）」が決定された。この政府統一基準に関しては適宜見直しが行われ、2015年2月現在、2014年5月に決定された「政府機関の情報セキュリティ対策のための統一基準（平成26年度版）」が運用されている。なお、2015年1月に施行されたサイバーセキュリティ基本法等に基づき、上記の事項も含め、情報セキュリティ政策会議の決定事項及び検討事項等はサイバーセキュリティ戦略本部に引き継がれた。

（2）　各府省庁の情報セキュリティ体制

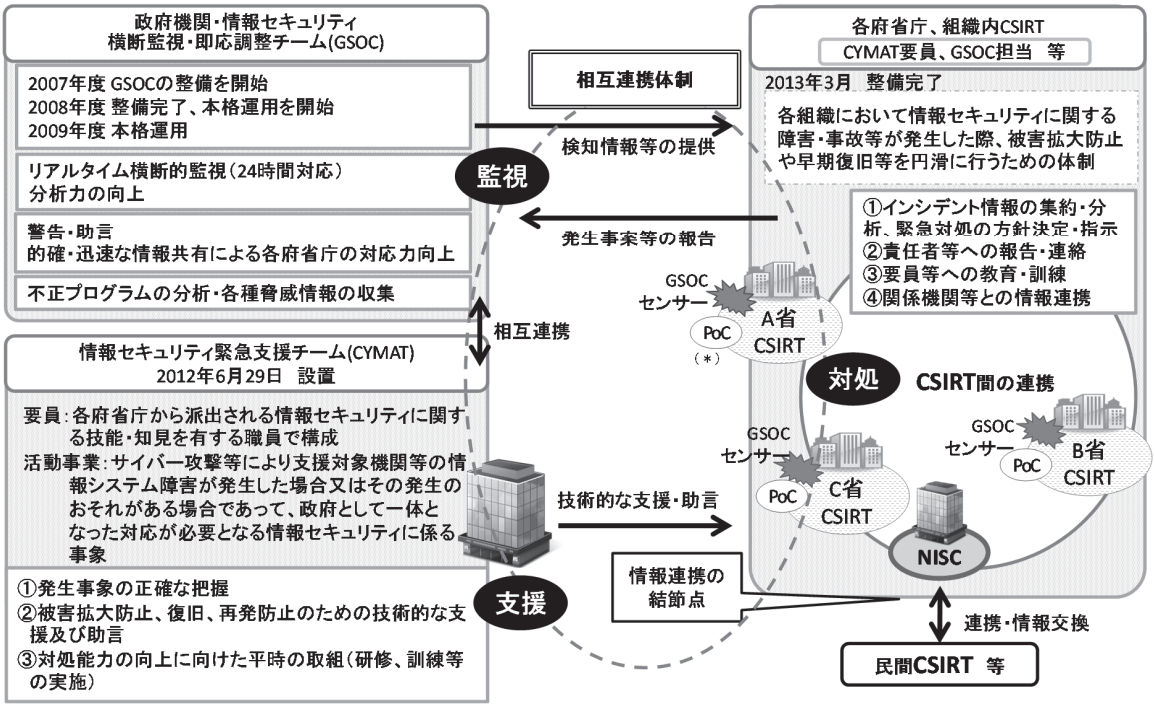
この統一基準は、各府省庁において整備すべき組織や体制について遵守事項を規定している。最高情報セキュリティ責任者（Chief Information Security Officer: CISO）が各府省庁において任命されている（多くの省庁では官房長が務める）。CISOは統一基準に準拠した府省庁対策基準等の審議を行うための情報セキュリティ委員会（部局の代表者を構成員とする）を設置し基準を策定するとともに、専門的助言を求めるため情報セキュリティの有識者である最高情報セキュリティアドバイザーを設置する。またCISOは、コンピュータやネットワーク上の問題発生の監視・分析・調査を行うために、発生したインシデントに対応する組織横断の専門チームCSIRT（Computer Security Incident Response Team）を府省庁内に整備する。CSIRTの構成員についてはCISOが選任する。後述するCYMATに属する職員についても、CISOが指名する。[(3)]

（3）　政府機関横断的組織

政府機関の横断的な組織として、政府機関監視・即応調整チーム（Government Security Operation Coordination Team: GSOC）及び情報セキュリティ緊急支援チーム（CYber incident Mobile Assistant Team: CYMAT）が設置されている（図1参照）。GSOCは2008年に運用が開始された。リアルタイムで府省庁横断的に攻撃を監視するとともに発見された電子政府の脆弱性に対して警告や助言を行い、政府機関全体の対応力向上を目的として活動している(4)。CYMATは、NISCの統括の下で、政府一体として対応が必要な事案について、復旧・被害拡大防止、原因調査、再発防止等のための技術的な支援及び助言を行うため、全府省庁から選任された情報セキュリティに関する技能・知見を有する職員で構成される組織として、2012年に設置された(5)。

各府省庁間の連携については2010年からCISOの機能強化の一環として最高情報セキュリティ責任者等連絡会議（情報セキュリティ対策推進会議）及び最高情報セキュリティアドバイザー等連絡会議を設置している(6)。これらの会議もNISCの下で運営されている。

図1　GSOC・CYMAT・CSIRTの連携体制



（＊）Point of Contactのこと。図中では各省庁の連絡窓口を指す。
（出典）情報セキュリティ政策会議「サイバーセキュリティ政策に係る年次報告（2013年度）」2014.7.10, p.15. <http://www.nisc.go.jp/active/kihon/pdf/jseval_2013.pdf>を基に三菱総合研究所作成。

●事例研究

■各府省庁における情報セキュリティの取組と推奨事例

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））は、2010年に全府省庁の協力を得ながら情報セキュリティ報告書（「政府機関における情報セキュリティに係る年次報告」）の作成を開始した(7)。当該報告書においては、一年間の全府省庁の取組の紹介・評価に留まらず、推奨事例として全府省庁が実施すべき取組を紹介している。最新版の「サイバーセキュリティ政策に係る年次報告（2013年度）」では最高情報セキュリティアドバイザー等連絡会議に基づく推奨事例の掲載はない。

2012年度報告書における推奨事例は3事例が選定されている。金融庁は、コピープリンタ複合機の情報セキュリティ監査対象機器への追加を行っている。近年の複合機はスタンドアローンの出力機器に留まらず、Webサーバ機能を搭載しネットワークシステムを構成することができる。しかし運用管理においては情報セキュリティを担当する部署以外の所管となることが多く、情報漏えいリスクやシステムの脆弱性が看過されてきた。複合機を情報セキュリティ監査対象機器に追加することでその情報セキュリティ上のリスクを認識し、対策を講じることが可能となった。外務省は、情報セキュリティ対策を学習するeラーニングに関して一定の期間以内に学習が終了しない場合に自動的にインターネット利用を制限する取組を行っている。経済産業省は、システムにおける本人認証強化を目的とした取組を行った。具体的には基盤情報システムへのログインの際に、複数要素主体認証（ID・パスワード・ICカード）を導入し、スマートフォンやタブレット等の端末からも安全に利用できる環境を整備した。この取組によって、第三者によるシステムの不正利用が困難になった。(8)

●海外の状況、技術動向、制度、規制

■米国連邦政府の情報セキュリティ対策

米国連邦政府における情報セキュリティ体制は、行政管理予算局（Office of Management and Budget: OMB）の予算管理のもと、米国国立標準技術研究所（National Institute of Standards and Technology: NIST）、司法省所管の連邦捜査局（Federal Bureau of Investigation: FBI）、国防総省所管の米国国家安全保障局（National Security Agency: NSA）や国防高等研究計画局（Defense Advanced Research Projects Agency: DARPA）、国土安全保障省（Department of Homeland Security: DHS）、また同省所管のサイバーセキュリティ通信統合センター（National Cybersecurity Communication Integration Center: NCCIC）やUS-CERT（United States Computer Emergency Readiness Team）等の組織が担っている。さらに、大統領府にはCTO（Chief Technology Officer）のほか、サイバーセキュリティ調整官（Cybersecurity Coordinator: CSC）が設置され、連邦政府機関のサイバーセキュリティの統括責任者として、連邦政府の情報セキュリティ政策を主導している。また、連邦政府の情報セキュリティ強化を目的とした連邦情報セキュリティマネジメント法（Federal Information Security Management Act of 2002: FISMA）が2002年に制定されており、規格やガイドラインの開発はNIST、連邦政府の取組状況の評価はOMBが実施している。

現在、連邦政府内の情報セキュリティ対策において中心的役割を担っているのがDHSである。DHSは2001年の米国同時多発テロの発生を受けて、2002年に設立された組織で、情報セキュリティを含めたあらゆる脅威から国土の安全を守ることを目的としている(9)。

DHSにおいて情報セキュリティインシデント対応を担当する組織がUS-CERTである。US-

CERTは2003年に設立され、コンピュータやネットワーク上の問題発生の監視・分析・調査を24時間体制で行い、連邦政府のCSIRTに相当する(10)。

サイバーセキュリティに関する研究や情報収集分析を行う組織としてカーネギーメロン大学で運営されているCERT/CC（CERT Coordination Center）が各国の連携を強化している。CERT/CCは米国の組織で、1988年にMorrisワーム事件（マルウェアの一種による攻撃が問題となった事件）を受けて発足した(11)。コンピュータやネットワーク上の問題発生の監視・分析・調査を行う組織であるCSIRTの草分けであり、US-CERTの設立においてはDHSに協力した。

CERT/CCは世界各国のNational CSIRT（日本においてはJPCERT/CC）と連携しており、毎年Annual Technical Meeting for CSIRTs with National Responsibilityを開催している。会議においては、国際的なインシデント（情報セキュリティを脅かす事態）の予防や対応、技術分析等に関する最新情報の交換を行っている(12)。

(1)　占部浩一郎「情報セキュリティ政策の概要」2012.9.8, p.1. マルチメディア振興センターウェブサイト <http://www.fmmc.or.jp/pdf/news/0908kouensiryou7.pdf>
(2)　「（参考）「政府機関の情報セキュリティ対策のための統一基準」について（過去の経緯）」内閣サイバーセキュリティセンターウェブサイト <http://www.nisc.go.jp/active/general/kijun26.html>
(3)　情報セキュリティ政策会議「政府機関の情報セキュリティ対策のための統一基準について（平成26年度版）」2014.5.19, pp.9-11. <http://www.nisc.go.jp/active/general/pdf/kijyun26.pdf>
(4)　占部　前掲注(1), p.3.
(5)　内閣官房情報セキュリティセンター「情報セキュリティ緊急支援チーム（CYMAT）設置について」2012.6.29. <http://www.nisc.go.jp/press/pdf/cymat_press.pdf>
(6)　情報セキュリティ対策推進会議「政府機関における情報セキュリティに係る年次報告（平成22年度）」2011.5.31, p.6. <http://www.nisc.go.jp/active/general/pdf/h22_report.pdf>
(7)　同上
(8)　情報セキュリティ対策推進会議「政府機関における情報セキュリティに係る年次報告（平成24年度）」2013.6.19, pp.30-31. <http://www.nisc.go.jp/conference/seisaku/dai36/pdf/36shiryou0402.pdf>
(9)　“History.”Department of Homeland Security Website <http://www.dhs.gov/history>
(10)　“About Us.”United States Computer Emergency Readiness Team Website <https://www.us-cert.gov/about-us>
(11)　“About Us.”CERT Coordination Center Website <http://www.cert.org/about/>
(12)　情報処理推進機構編『2014情報セキュリティ白書―もはや安全ではない：高めようリスク感度―』情報処理推進機構, 2014, p.87.

5.1.3　オープンデータ政策

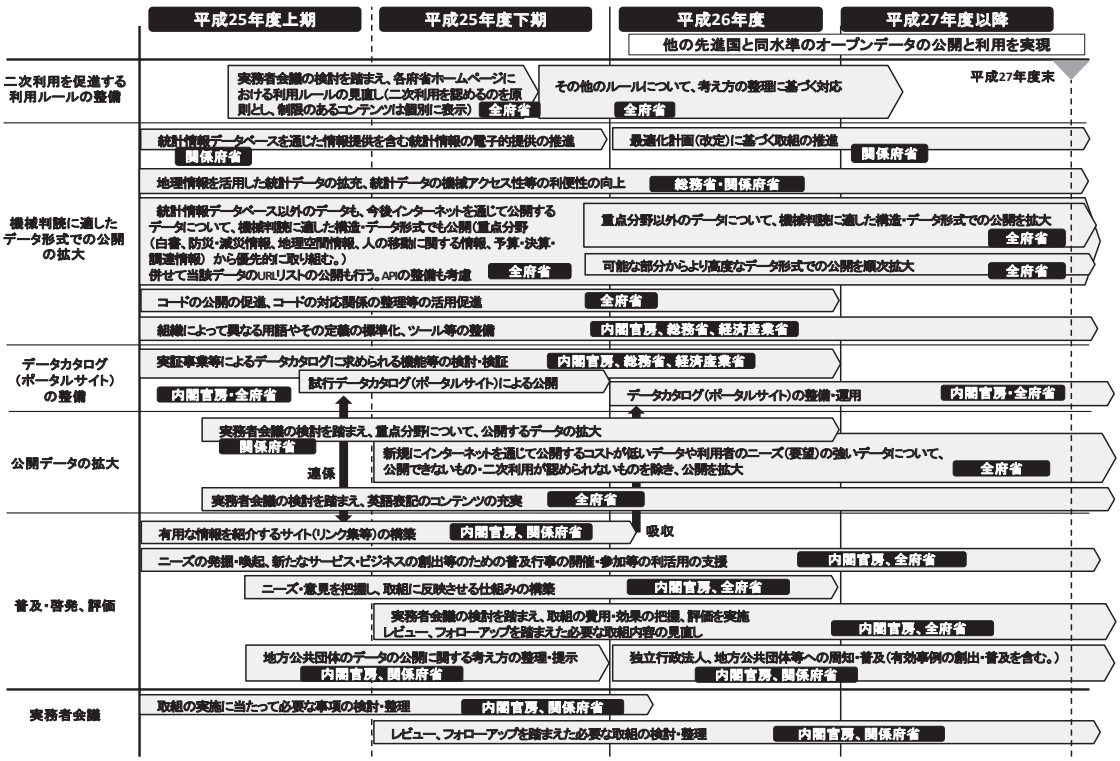
電子行政オープンデータ政策は、①行政の透明性・信頼性向上、②国民の公共データ活用ニーズの把握による国民参加・官民協働の推進、③ビジネス創出による経済活性化・行政効率化を目的として推進されているが、情報セキュリティ上の課題も抱えている。

(1)　電子行政オープンデータ政策とロードマップ

近年、「ブロードバンドの普及及び端末の能力向上・多様化（企業や国民が容易に大量なデータを扱える環境に）、ICT政策は「縦軸」から「横軸」の取組強化へ（東日本大震災では情報の横の連携の重要性が顕在化）、国、自治体、独立行政法人、公益事業者等が保有する公共データのビジネス活用等への期待の高まり」[(1)]等を背景として国・自治体・独立行政法人・公益事業者等が保有する多様な公共データを開放するオープンデータ政策が進められている。

政府では、オープンデータの条件を、①機械で判読可能なデータ形式で、②二次利用が可能な利用ルールで公開されるデータ、としている[(2)]。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、現：IT総合戦略本部）が「電子行政オープンデータ戦略」（2012年7月4日高度情報通信ネットワーク社会推進戦略本部決定）を定めており、公共データは国民共有の財産であるとの認識の下、公共データの活用を促進することが重要とされている[(3)]。2013年6月には「電子行政オープンデータ推進のためのロードマップ」をIT総合戦略本部が決定した（図1参照）[(4)]。本ロードマップによれば、2015年度末をターゲットとして、オープンデータの公開と利用を促進し、他の先進国と同レベルに達することを目標としている。

図1　電子行政オープンデータ推進のためのロードマップ



（出典）高度情報通信ネットワーク社会推進戦略本部「電子行政オープンデータ推進のためのロードマップ」2013.6.14. <http://www.kantei.go.jp/jp/singi/it2/kettei/pdf/20130614/siryou3.pdf>を基に三菱総合研究所作成。

(2)　オープンデータに関する基盤整備等

現在、総務省及び経済産業省等を始めとする関係府省から構成される、電子行政オープンデータ実務者会議において、情報基盤の構築や情報公開技術・制度の提供が進められている[5]。2012年には総務省が中心となり、産学官が共同でオープンデータ流通環境の実現に向けた基盤整備を推進することを目的として、「オープンデータ流通推進コンソーシアム」が設立された。同コンソーシアムは、2014年に「オープン＆ビッグデータ活用・地方創生推進機構」に移行した。2015年2月現在、134組織が参加している。同機構では、①公共機関の積極的なデータの公開、②民間保有データとの組合せにより新たなデータを作成することを考慮したデータ形式の標準化、③民間保有データのうち公共性の高いものの流通・活用などを促進するため、公共機関保有データと民間保有データの間をつなぐためのオープンデータの利用ルールや技術に関する検討及び普及啓発活動に取り組んでいる[6]。

(3)　オープンデータ政策における課題

オープンデータ政策における具体的な課題としては、第一に著作権侵害が考えられる[7]。オープンデータは二次利用可能を定義要件としており、省庁が作成した統計データ等では基本的には問題は生じないが、省庁が刊行する白書等においては第三者の著作物が掲載される場面も多い。この問題については、各府省情報化統括責任者（CIO）連絡会議が2013年6月25日に決定した「二次利用の促進のための府省のデータ公開に関する基本的考え方（ガイドライン）」に府省庁のデータ利用に関する統一的な考え方が定められ[8]、オープンデータ推進に向けた取組が進められている。すなわち、主な利用ルールの在り方として、①データについて著作権の保護対象外であることの明確化、②国が著作権者である著作物は広く二次利用を認め、統一的な表示を実施、③著作権を根拠に二次利用を制限する場合、理由及び範囲の国による明確な表示、④各府省が新たに作成・入手するデータについては、二次利用可能なように事前に関係者間で合意を形成、などが示された。また、各府省ホームページの利用ルールの見直しのひな形として「政府標準利用規約（第1.0版）」を作成した[9]。

第二にプライバシーの問題が考えられる。個々の統計データにおいて匿名性が確保されていても、複数のデータの組合せによって個人の特定が可能になるおそれがある。

第三に、データの二次利用における情報の改ざんの可能性も考えられる[10]。オープンデータは二次利用による新規ビジネスの創出を可能とするが、二次利用の過程において数値の改ざんや恣意的な演算が行われるとデータそのものの「完全性」が損なわれる。これは情報セキュリティ三要素の中の「完全性」に関するリスクである。

最後に、オープンデータ公開ウェブサーバの安全性が問題となる。ウェブサーバがハッキング等の攻撃を受けて情報が改ざん又は情報へのアクセスが不可能になると、「完全性」及び「可用性」が損なわれる結果となる。

●事例研究

■国内におけるオープンデータ活用事例

IT総合戦略本部の主導の下、国全体でのオープンデータ公開に向けた検討・整備が進められており、2014年10月1日には、内閣官房のデータカタログサイト「DATA.GO.JP」が稼働した。同サイトは企業や個人向けに行政機関が保有している二次利用が可能な公共データの案内・横断的検索サービスを提供することを目的としており、構築及び運用には日立製作所が提供する「オープンデータソリューション」を利用している(11)。

また、個別の自治体でも先行的な取組が実施されている(12)。横浜市では、独自のオープンデータカタログサイトを整備し、2015年2月時点で試行版として公開している(13)。また、全国4市（佐賀県武雄市、千葉市、奈良市、福岡市）が中心となったビッグデータ・オープンデータ活用推進協議会では、公共データ等の活用について、シンポジウムの開催を通じて検討を行っている。そのほかホームページ上での公共データのオープン化については、既に複数の自治体が実施している。

オープンデータの活用事例としては、ウェブサイト「Where Does My Money Go?　税金はどこへ行った？」がある(14)。同ウェブサイトは、英国のオープンデータ推進団体Open Knowledge Foundationが開発した同名のサービスを利用しており、税金の用途を可視化し、オープンデータ政策のうち「行政の透明性向上」に資する。その後このサービスは全国各地での利用が進み、160を超える自治体において運用されている。また「復旧復興支援ナビ」(15)は、国や自治体が行っている支援制度を復旧復興支援制度データベースに集約し、統一書式で情報を提供し、民間の支援情報を付加して情報提供していた（2015年2月10日現在では民間支援情報の登録はない）。行政の透明性向上及び官民協働の事例といえる。

●海外の状況、技術動向、制度、規制

■米国のオープンデータ政策

米国では、オバマ大統領が就任直後の2009年1月に覚書「透明性とオープンガバメント（Transparency & Open Government）」(16)を発出し、「透明性（Transparency）」、「国民参加（Participation）」、「協業（Collaboration）」の三原則に基づき、開かれた政府を築くことを表明している。その後連邦政府は2009年にオープンデータを公開するウェブサイトData.gov(17)を開設した。(18)

また、2012年5月に発表された「デジタルガバメント戦略（Digital Government: Building a 21st Century Platform to Better Save the American People）」では、数値データに加え文書情報等もオープンガバメントの対象としている。(19)

2013年5月には政府情報のオープンデータ化を義務付ける大統領令（Making Open and Machine Readable the New Default for Government Information, Executive Order 13642）を制定し、あわせて大統領府の科学技術政策局（Office of Science and Technology Policy: OSTP）、行政管理予算局（Office of Management and Budget: OMB）等が政府機関によるオープンデータの公開方針を示す覚書（Open Data Policy-Managing Information as an Asset）を公表している(20)。

2014年5月には米国初のオープンデータ関連の法律として、データ法（The Digital Accountability and Transparency Act of 2014: DATA Act）が成立し、連邦政府の支出のデータの公開が義務化された(21)。

2014年9月時点で顕在化したリスクとしては、オープンデータの継続的な提供が挙げられる。

2013年10月1日から発生した一部政府機関の閉鎖の際、オープンデータのウェブサイトであるData.govも閉鎖された(22)。それに伴い、気象データや交通データ等のリアルタイムで更新されるデータの公開も停止された。結果として、これらのリアルタイムデータを活用する事業者がサービス提供に支障をきたす事態となった。

(1)　「オープンデータとは」総務省ウェブサイト <http://www.soumu.go.jp/menu_seisaku/ictseisaku/ictriyou/opendata/opendata01.html>
(2)　高度情報通信ネットワーク社会推進戦略本部「電子行政オープンデータ推進のためのロードマップ」2013.6.14, p.1. <http://www.kantei.go.jp/jp/singi/it2/kettei/pdf/20130614/siryou3.pdf>; オープンデータ流通推進コンソーシアム「オープンデータガイド―オープンデータのためのルール・技術の手引き―第1版」2014.7.31, p.16. <http://www.opendata.gr.jp/news/docs/opendata-guide-v1.pdf>
(3)　高度情報通信ネットワーク社会推進戦略本部「電子行政オープンデータ戦略」2012.7.4, p.1. <http://www.kantei.go.jp/jp/singi/it2/pdf/120704_siryou2.pdf>
(4)　高度情報通信ネットワーク社会推進戦略本部　前掲注(2)
(5)　経済産業省商務情報政策局情報プロジェクト室「オープンデータに関する経済産業省の取組」2012.12. <http://www.kantei.go.jp/jp/singi/it2/densi/dai1/siryou8.pdf>; 総務省「オープンデータに関する総務省の取組―情報流通連携基盤の構築、オープンデータ流通推進コンソーシアム等―」2012.12.10. <http://www.kantei.go.jp/jp/singi/it2/densi/dai1/siryou7.pdf>
(6)　「機構について」オープン＆ビッグデータ活用・地方創生推進機構ウェブサイト <http://www.vled.or.jp/about/purpose/>
(7)　株式会社公共イノベーション「平成24年度情報セキュリティ対策推進事業（オープンデータ推進における情報リスク対策に関する調査研究）報告書」2013.3.22, p.7. <http://www.meti.go.jp/meti_lib/report/2013fy/E003379.pdf>
(8)　「二次利用の促進のための府省のデータ公開に関する基本的考え方（ガイドライン）」2014.6.19, pp.4-5. 首相官邸ウェブサイト <http://www.kantei.go.jp/jp/singi/it2/densi/kettei/data/gl26_honbun.pdf>
(9)　電子行政オープンデータ実務者会議「政府標準利用規約（第1.0版）」首相官邸ウェブサイト <http://www.kantei.go.jp/jp/singi/it2/densi/dai7/sankou2.pdf>
(10)　株式会社公共イノベーション　前掲注(7), p.11.
(11)　「日立の「オープンデータソリューション」を活用した内閣官房のデータカタログサイト「DATA.GO.JP」が稼働開始―行政機関が保有するオープンデータの横断的な検索を実現し、活用を推進―」2014.9.30. 日立製作所ウェブサイト <http://www.hitachi.co.jp/New/cnews/month/2014/09/0930a.html>
(12)　経済産業省「オープンデータの活用事例―海外及び日本の事例―」2014, pp.15-16. <http://datameti.go.jp/wp-content/uploads/2014/01/03b558b1126807662402d3ebb9a98605.pdf>
(13)　「よこはまオープンデータカタログ（試行版）」横浜市ウェブサイト <http://www.city.yokohama.lg.jp/seisaku/seisaku/opendata/catalog.html>
(14)　「Where Does My Money Go? 税金はどこへ行った？」横浜市ウェブサイト <http://yokohama.spending.jp/>
(15)　復旧復興支援ナビウェブサイト <http://www.fsnavi.jp/Simin/Index.aspx>
(16)　Transparency and Open Government（Memorandum for the Heads of Executive Departments and Agencies）, 74 FR 4685（2009.1.26.）
(17)　Data.Gov Website <https://www.data.gov/>
(18)　総務省編「第1部第2章第1節電子行政とオープンデータ」『平成25年版情報通信白書―ICT白書―』日経印刷, 2013.7, p.204. <http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h25/pdf/25honpen.pdf>
(19)　同上
(20)　Executive Office of the President and Office of Management and Budget,“Memorandum for the Heads of Executive Departments and Agencies: Subject: Open Data Policy-Managing Information as an Asset,”May 9, 2013. <http://www.whitehouse.gov/sites/default/files/omb/memoranda/2013/m-13-13.pdf>
(21)　大槻文彦「オープンデータの最新動向―米連邦「データ法」が開く世界―」2014.7.11. 富士通総研ウェブサイト <http://www.fujitsu.com/jp/group/fri/column/opinion/201407/2014-7-1.html>
(22)　“The shutdown is now clogging up the data economy. Thanks, Congress!”*Washington Post*, October 3, 2013. <http://www.washingtonpost.com/blogs/the-switch/wp/2013/10/03/the-shutdown-is-now-clogging-up-the-data-economy-thanks-congress/>

5.1.4　インターネットを利用した選挙

日本では2013年5月26日に施行された改正公職選挙法により、選挙運動期間における候補者に関する情報の充実、有権者の政治参加の促進等を図るため、インターネット等を利用した選挙運動が解禁された。

「公職選挙法」（昭和25年法律第100号）は、選挙の公正、候補者間の平等を確保するため、選挙運動期間中に行われる文書図画の頒布・掲示その他の選挙運動について一定の規制を行ってきた。ホームページや電子メール等のインターネット等を利用した情報の伝達も文書図画の頒布に当たるものとして規制されてきた。一方、諸外国では、手法等に多少の制限を設ける国はあるものの、既にインターネットが広く選挙活動に利用されている(1)。

国内でもインターネット等を利用した選挙の解禁に対する議論が高まり、2013年5月26日に施行された「公職選挙法の一部を改正する法律」（平成25年法律第10号）によりウェブサイト等及び電子メールを利用する方法による選挙運動用の文書図画の頒布が一部の制限のもと解禁されることとなった。

ウェブサイト等の利用に関しては、誰でもウェブサイト等（ホームページ、ブログ、SNS、動画共有サービス、動画中継サイト）を利用する方法により、選挙運動を行うことができるようになった。ただし、選挙運動用ウェブサイト等には電子メールアドレス等の連絡に必要となる情報を表示することが義務付けられる。また、ウェブサイト等に掲載された選挙運動用文書図画は、選挙期日当日もそのままにしておくことができるが、選挙運動は選挙期日の前日までに限られており、選挙期日当日にウェブサイトを更新することはできない。(2)

電子メールの利用に関しては、候補者・政党等に限って、選挙運動用文書図画を電子メールにより頒布することができるようになった。なお、候補者・政党等以外の一般有権者は引き続き禁止されている。また、選挙運動用電子メールの送信に当たっては、送信先に一定の制限が設けられ、電子メール送信者には、一定の記録の保存（受信者からの電子メールや送信の申込書面、メールマガジンの送信先リスト等）と、送信される文書図画には送信者の氏名・名称やメールアドレス等、一定の事項を表示することが義務付けられる。(3)

そのほか、選挙運動のための有料インターネット広告の禁止（ただし、政党等は選挙期間中、当該政党等の選挙運動用ウェブサイト等に直接リンクする政治活動用有料広告を掲載することができる。）、インターネット等を利用した選挙期日後の挨拶行為の解禁、屋内の演説会場内における映写等の解禁も併せて行われた。(4)

候補者への誹謗中傷・なりすまし対策については、既存の公職選挙法、「刑法」（明治40 年法律第45 号）、「不正アクセス行為の禁止等に関する法律」（いわゆる「不正アクセス禁止法」。平成11年法律第128号）により刑罰が設けられているが、改正公職選挙法により氏名等の虚偽表示罪の対象としてインターネット等による通信が追加されたほか、「特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律」（いわゆる「プロバイダ責任制限法」。平成13年法律第137号）に、選挙運動又は当選を得させないための活動に使用する文書図画によって自己の名誉を侵害されたとする候補者・政党等からの申出を受けたプロバイダ等の対応について、①プロバイダ等から情報発信者に対する削除同意照会期間を通常の7日から2日に短縮、②

電子メールアドレス等の表示義務を果たしていない情報については、情報発信者に照会せず直ちに削除しても民事上の賠償責任は問われない、とする特例が設けられた。(5)

●事例研究

■2013年参院選

改正公職選挙法施行後初の国政選挙となった2013年参院選では各党がインターネットを利用した選挙運動を展開した。Google日本法人、慶應義塾大学曽根泰教教授、調査会社のインテージ、ビッグデータ分析会社のブレインパッドが共同で、関東圏の20～69歳の男女約2,400人を対象に2013年5月から7月と選挙後の7月22日に実施した参院選における有権者の投票行動とネットやテレビの閲覧状況との関連性調査の結果によれば、各政党の公式サイトの訪問率はほとんどの政党で1%を大きく下回っていた。また、政治情報を得るためのネットやテレビの閲覧状況は、全体の95%がテレビ番組を利用しているのに対し、ウェブサイトを利用している人の割合は41%であり、選挙においてインターネットが有権者に十分に活用されていない状況が明らかとなり、今後のネット選挙の在り方について、課題を残すこととなった。(6)

●海外の状況、技術動向、制度、規制

■米国大統領選挙キャンペーンにおけるソーシャルメディアの利用

米国では、2008年の大統領選挙キャンペーンにおいてオバマ大統領候補（当時）が特設のSNSである“My.barackobama.com”を利用して支援者のネットワークを広げ、さらにSNSを通じた献金を導入したことにより潤沢な選挙資金を獲得した。以後選挙キャンペーンにおけるソーシャルメディアの利用が広く普及した。2012年の大統領選挙キャンペーンでは、両陣営とも公式サイトのほか、主要SNS（Facebook, Twitter, YouTube, Flickr, Google+等）を通じて選挙キャンペーンを展開した。両候補とも公式サイトをFacebookと連動させ、Facebookの登録情報を利用したことで、選挙キャンペーンを低コストで展開することが可能となった(7)。

米国シンクタンクのPew Research Center の調査によれば、米国人が2012年選挙キャンペーンの情報を得るのに日常的に使った情報源は、TVのケーブルニュース41%、ローカルニュース38%、インターネット36%、地方紙23%、全国紙13%、NPR（National Public Radio）12%、Facebook12%、YouTube7%、Twitter4%等となっており、SNSが有権者の情報源として実際に活用されている。同調査では、1つの選挙キャンペーンの情報源のみを利用していると回答した人は全体の6%に過ぎず、多様なメディアからの情報収集が定着している状況がうかがえる。また、SNSを使って家族や友達から、投票するように促されたと回答した有権者の割合は18～29歳では45%、30～49歳では40%、50～64歳では27%、65歳以上では11%と、特に若い世代においてSNSを使った選挙に関する情報共有が浸透している。(8)

(1)　三輪和宏「諸外国のインターネット選挙運動」『調査と情報―ISSUE BRIEF―』518号, 2006.3.6, p.10. <http://dl.ndl.go.jp/view/download/digidepo_1000670_po_0518.pdf?contentNo=1>
(2)　総務省「インターネット選挙運動解禁（公職選挙法の一部を改正する法律）の概要」pp.4-5. <http://www.soumu.go.jp/main_content/000224709.pdf>
(3)　同上, pp.6-11.
(4)　同上, pp.12-14.
(5)　同上, pp.16-19.
(6)　杉原梓「初のネット選挙は「肩すかし」 候補者サイト閲覧は1%　グーグル日本法人などがビッグデータ解析」『日本経済新聞』（電子版Tech Frontline）2013.7.30. <http://www.nikkei.com/article/DGXNASFK30015_Q3A730C1000000/>
(7)　“Obama, Facebook and the power of friendship: the 2012 data election,”*Guardian*, February 17, 2012. <http://www.theguardian.com/world/2012/feb/17/obama-digital-data-machine-facebook-election>
(8)　Pew Research Center,“Digital Politics: Pew Research findings on technology and campaign 2012,”February 20, 2013. <http://www.pewinternet.org/2013/02/20/digital-politics-pew-research-findings-on-technology-and-campaign-2012/>

5.2　確保されるべき権利・利益

5.2.1　秘密保護

秘密保護はサイバーセキュリティを考えるうえで重要な要素となっている。我が国における主な秘密保護関連法としては、特定秘密保護法、不正競争防止法等がある。

情報がデジタル化されることは利便性を高めた一方、その漏えい等の危険も増大させたことで、秘密保護はサイバーセキュリティを考えるうえで重要な要素となっている。

我が国における安全保障関連の秘密情報保護関連法には、防衛・安全保障・外交等に関する情報保護を定めた「特定秘密の保護に関する法律」（いわゆる「特定秘密保護法」。平成25年法律第108号）、公務員が職務上知り得た秘密を保護するための「国家公務員法」（昭和22年法律第120号）、防衛秘密の秘密保全を定めた「自衛隊法」（昭和29年法律第165号）、米国から供与された装備品等に関する秘密保護を定めた「日米相互防衛援助協定等に伴う秘密保護法」（いわゆる「防衛秘密保護法」。昭和29年法律第166号）、日米地位協定に基づき米国軍隊の機密保全を定めた「日本国とアメリカ合衆国との間の相互協力及び安全保障条約第6条に基づく施設及び区域並びに日本国における合衆国軍隊の地位に関する協定の実施に伴う刑事特別法」（いわゆる「刑事特別法」。昭和27年法律第138号）がある。

2013年12月に成立、2014年12月に施行された特定秘密保護法は、行政機関の長が指定する特定秘密（防衛、外交、テロリズムの防止、スパイ行為等の防止に関する情報であって、公になっていないもののうち、安全保障上の著しい支障を与えるおそれがあるため、特に秘匿することが必要であるもの）について、取扱者の制限を行うとともに、これを漏えいした者等の処罰を定めた法律である。特徴としては、取扱者の制限を行うため適性評価を行うことを定めていることが挙げられる。なお取扱者は主に行政機関の職員、都道府県警察の職員であるが、契約履行のために特定秘密を提供された民間の契約業者の役職員も対象となる(1)。

特定秘密保護法の立法過程においては、国民の知る権利との関係で様々な議論がなされた。

安全保障以外の秘密情報保護関連法として、主に事業者が管理する営業秘密の保護を目的とした「不正競争防止法」（平成5年法律第47号）がある。不正競争防止法は、事業者間の公正な競争及びこれに関する国際約束（パリ条約、マドリッド協定等）の的確な実施を確保するため、不正行為類型の一つとして営業秘密の不正取得・不正使用を禁止している。①秘密管理性（秘密として管理されていることをいい、情報にアクセスできる者が制限されていること、情報にアクセスした者が秘密であると認識できることが必要とされる。）、②営業上又は技術上の有用性、③非公知性の3条件を満たすことが本法における保護の対象となる営業秘密の要件である。不正取得とは、窃取、詐欺、強迫その他の不正の手段により営業秘密を取得する行為であり、不正使用とは取得した営業秘密を自己又は第三者の利益を図り又は他人に損害を与える目的で使用又は開示する行為である。不正競争防止法の特色として、営業秘密の侵害に対して、民事的措置と刑事的措置（刑事罰）の両方を定めていることが挙げられる。経済産業省では不正競争防止法の要件を満たす営業秘密の管理の在り方について「営業秘密管理指針」を策定し、企業における営業秘密管理体制の構築等を求めている。刑事罰の拡大や被害企業の立証負担の軽減等を骨子とし

た不正競争防止法の改正が検討されている。

●事例研究

■ヤマザキマザック事件

工作機械メーカー大手のヤマザキマザックの中国籍社員が同社サーバにアクセスし、私物のハードディスクに秘密情報（工作機械の設計情報）を複製したとして、2012年3月27日に愛知県警は同社員を不正競争防止法違反（営業秘密侵害）容疑で逮捕した。同事件は、不正競争防止法の2009年改正で導入された不正の利益を得る目的での情報の取得に対する刑事罪が初めて適用された点や、2011年改正で導入された刑事訴訟手続の特例（営業秘密を保護するための秘密保持命令やインカメラ審理等）が適用された初めての裁判例となった。2014年8月20日、同社員に対する判決公判が名古屋地裁であり、懲役2年、執行猶予4年、罰金50万円の判決が言い渡された。なお、被告の社員は即日控訴している。(2)

■国内の企業における技術流出発生状況

経済産業省の委託調査（2012年度）によれば、過去5年間に回答企業の13.5%（全規模・全業種、非製造業も含む。）で人材を通じた何らかの営業秘密の漏えい事例があった(3)。

●海外の状況、技術動向、制度、規制

■米国の営業秘密保護政策

米国においては、1996年経済スパイ法（Economic Espionage Act of 1996, P.L.104–294）を制定し、営業秘密の不正取得を禁止している。同法では経済スパイ（外国政府による又は外国政府に便益を与えるための営業秘密の不正取得）と民間の個人・企業等による営業秘密の不正取得の両方を禁止している。なお、米国では民法一般に関する権限が連邦政府ではなく、州政府にあるため、経済スパイ法は、原則として刑事的側面だけを定めている(4)。なお、営業秘密保護強化のため、経済スパイ法改正案が提案されており、経済スパイの対象の拡大や営業秘密の定義の拡張などが検討されている(5)。

また、2013年2月には大統領府が中心となって取りまとめた「営業秘密侵害を低減するための米国政府戦略」が公表された(6)。同戦略では、①海外における営業秘密保護のための外交上の取組、②企業による自己防衛の促進、③司法当局による捜査や摘発、④法改正の検討、⑤広報・啓発活動等に関する米国政府の方針が盛り込まれている。

---

(1)　内閣官房「特定秘密の保護に関する法律案 説明資料」2013.10.25, pp.1-2. <http://www.cas.go.jp/jp/houan/131025/gaiyou.pdf>
(2)　「ヤマザキマザック機密取得　中国籍元社員に有罪　名古屋地裁」『日本経済新聞』2014.8.21.
(3)　三菱UFJリサーチ＆コンサルティング「人材を通じた技術流出に関する調査研究報告書（別冊）「営業秘密の管理実態に関するアンケート」調査結果」2013.3, p.50. <http://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/H2503chousa.pdf>
(4)　経済産業政策局知的財産政策室「営業秘密の要件各国対比表」（産業構造審議会知的財産分科会第1回営業秘密の保護・活用に関する小委員会資料7別紙2）2014.9.30. <http://www.meti.go.jp/committee/sankoushin/chitekizaisan/eigyohimitsu/pdf/001_07_02.pdf>
(5)　三菱総合研究所「諸外国における営業秘密保護制度に関する調査研究報告書」2014.3, pp.8-10. 経済産業省ウェブサイト <http://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/H25FYshogaikokuchosa.pdf>; Brian T. Yeh,“Protection of Trade Secrets: Overview of Current Law and Legislation,”*Congressional Research Service*, R43714, September 5, 2014. <http://fas.org/sgp/crs/secrecy/R43714.pdf>
(6)　Executive Office of the President,“Administration Strategy on Mitigating the Theft of U.S. Trade Secrets,” February 2013. <http://www.whitehouse.gov/sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf>

5.2.2　個人情報保護

個人情報の保護のため、我が国では2003年に個人情報保護法が成立した。個人のプライバシーを保護しつつ、ビッグデータの利活用を促進するため、個人情報保護の見直しに関する議論がIT総合戦略本部の「パーソナルデータに関する検討会」を中心に行われ、2014年6月には「パーソナルデータの利活用に関する制度改正大綱」が決定された。

法制の中でプライバシー保護の考えが登場したのは、1950年に調印され1953年に発効した「人権と基本的自由の保護のための条約（欧州人権条約）」の第8条にプライバシーの保護が盛り込まれたのが最初といわれる。その後、1969年にドイツのヘッセン州が世界で初めての個人情報保護法を制定した(1)。1980年には経済協力開発機構（Organisation for Economic Co-operation and Development: OECD）がOECDプライバシーガイドラインを策定し(2)、プライバシー保護に関する基本的な考え方、いわゆるOECD8原則を示したことを一つの契機に、我が国においてもプライバシー保護に関する意識が高まった(3)。なお、プライバシーと個人情報は似たような概念として捉えられることも多いが、その対象範囲は若干異なることに留意が必要である(4)。

地方自治体における先行的な取組の後、政府においても行政機関を対象とした「行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律」（昭和63年法律第95号）が1988年に制定された。翌1989年には、通商産業省（現：経済産業省）が民間部門を対象とした「民間部門における電子計算機処理に係る個人情報の保護に関するガイドライン」（平成9年通商産業省告示第98号）を策定している。

1995年にはEU加盟国における個人データの保護水準を平準化するため、「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」。）が制定された。この指令の中では、個人データ(5)の保護が不十分なEU域外の第三国に対する個人情報の移転を制限する旨の規定が盛り込まれていたことから、我が国においても欧州と同等の保護措置を講ずるべきとの機運が生じた。加えて2000年前後に発生した個人情報漏えい事件や、インターネットの普及に伴う電子商取引の拡大等を契機に、民間事業者を対象とした法整備が行われることとなった。こうした背景を経て、「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）が2003年に成立し、2005年に全面施行された。

一方、学校や会社の緊急連絡網が作れない、災害時の要援護者名簿が作れない、統計調査に協力が得られないなどの「過剰反応」が発生しているともいわれる(6)。また、いわゆるビッグデータ等、個人情報保護法制定当時には想定されていなかった利活用が行なわれるようになってきたことから、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）の「パーソナルデータに関する検討会」を中心に個人情報保護の見直しに関する議論が行なわれた。2014年6月には「パーソナルデータの利活用に関する制度改正大綱」がIT総合戦略本部によって決定された。同大綱では、「個人の特定性を低減したデータ」の第三者提供は本人同意を不要とするとともに、現在各主務大臣がもつ個人情報取扱事業者に対する機能・権限に加え、立入検査等の機能・権限をもつ独立した第三者機関の体制を整備する旨が示された(7)。これは、我が国が独立した第三者機関を備えていないため、EUデータ保護指令に抵触し、EUからの個人データの第三国移転に支障が生じていることを受けている。政府は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。

関連する取組として、2013年に成立した「行政手続における特定の個人を識別するための番号の利用等に関する法律」（いわゆる「番号法」。平成25年法律第27号）に基づき、特定個人情報（マイナンバーを含む個人情報）の取扱を監視・監督するため、独立した第三者機関である「特定個人情報保護委員会」が2014年1月に設立された。ただし、同委員会は個人情報保護やプライバシー保護の全般を所掌するものではない。

●事例研究

■ベネッセ個人情報漏えい事件

教育サービスを提供するベネッセコーポレーションの顧客情報が、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により持ち出され、名簿業者に販売され、約3500万件の個人情報が漏えいしたとされる(8)。2014年7月17日、警視庁は業務委託先の社員を不正競争防止法違反の容疑で逮捕した(9)。また被害者による集団訴訟も起こされている。

同社では漏えいした顧客へのお詫びとして500円の金券を配布するとともに、再発防止策として、技術的な対策を講じ、業務委託先の管理の強化、グループ全体の情報管理体制・組織改革、外部監視機関の設置等を行うこととしている。2014年9月26日、経済産業大臣は個人情報保護法第34条第1項の規定に基づき、法違反行為を是正するために必要な措置をとり、個人情報の漏えいの再発防止を徹底するよう、同社に対して勧告した。

●海外の状況、技術動向、制度、規制

■EUデータ保護指令とEU データ保護規則

1995年に採択されたEUデータ保護指令に基づきEU加盟国は国内法を整備してきたが、ばらつきがあることが問題となっていた。これに対して、一段と強制力のあるEUデータ保護規則の策定が進んでいる。欧州議会が第一読会として2014年3月12日に決議し、欧州理事会に送られた「EUデータ保護規則案」にはEU域外へのデータ持出しを従来以上に規制することや、データの対象者が自身の個人データを消去することを求めることができる権利である「消去権」等が盛り込まれている(10)。EUにおける立法は議会と理事会の合意によるものであるため、今後、欧州理事会との協議を行い、最終案を2015年にまとめることを目指している。

(1)　消費者庁「諸外国等における個人情報保護制度の実態調査に関する検討委員会報告書」2009.3, p.112. <http://www.caa.go.jp/planning/kojin/h21report3.pdf>
(2)　Organisation for Economic Co-operation and Development,“OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,”September 23, 1980. <http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm>（同ガイドラインは2013年7月に改正。）
(3)　堀部政男「1980年OECDプライバシーガイドラインと日本」2013.12, pp.9-23. 日本情報経済社会推進協会ウェブサイト <http://www.jipdec.or.jp/publications/oecd/1980oecd.pdf>
(4)　「よくわかるプライバシーマーク制度―「個人情報」と「プライバシー」の違い―」日本情報経済社会推進協会ウェブサイト <http://privacymark.jp/wakaru/kouza/theme1_03.html>
(5)　EUデータ保護指令における「個人データ」は個人に関する全ての情報と定義されている。一方、日本の個人情報保護法における「個人情報」とは特定の個人を識別できる情報と定義されている。
(6)　小暮純也「統計調査と個人情報保護」『統計Today』No.7, 2009.6.4. <http://www.stat.go.jp/info/today/007.htm>
(7)　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, pp.10, 13-15. <http://www.kantei.go.jp/jp/singi/it2/info/h260625_siryou2.pdf>
(8)　「事故の経緯」ベネッセコーポレーションウェブサイト <http://www.benesse.co.jp/customer/bcinfo/01.html>
(9)　個人情報保護法違反でないのは、個人情報保護法が対象としているのは事業者であるためである。
(10)　European Union,“Progress on EU data protection reform now irreversible following European Parliament vote(MEMO/14/186),”March 12, 2014. European Commission Website <http://europa.eu/rapid/press-release_MEMO-14-186_en.htm>

5.2.3　デジタルコンテンツと著作権保護

インターネット上のコンテンツやデジタルデータも著作権の保護の対象であり、著作権者の権利を侵害せずに活用しなければならない。近年、コンテンツのデジタル化・ネットワーク化に伴う新サービスの提供が加速し、新たな著作権侵害の発生が問題となっている。

著作権は知的財産権の一つであり、著作物を創作する著作者の権利である。「著作権法」（昭和45年法律第48号）は、これらの著作物の保護と公正な利用の両立を図ることにより文化の発展に寄与することを目的としている。

著作権法で保護される著作物は「思想又は感情を創作的に表現したものであつて、文芸、学術、美術又は音楽の範囲に属するもの」と定義されている（著作権法第2条第1項第1号）。ブログやホームページに掲載した自己の文章や絵、画像データ等は上記の定義を満たせば著作物として保護される。また、コンピュータプログラムについては著作権法第2条第1項第10号の2により「プログラムの著作物」として保護される。一方で、統計調査等の単純なデータや数値は、定義のうち「思想又は感情」に該当しないため、著作物として保護されない。データ等を集約したデータベースについては著作権法第2条第1項第10号の3により「データベースの著作物」として保護される。ただし、データベースについては同条文が「その情報の選択又は体系的な構成によつて創作性を有するもの」と定義しているため、素材の選択や配列がありふれたものは著作物に当たらない。データベースについては全体に著作権が認められ、その内部のデータに関する個々の著作権とは別個の著作権が発生する(1)。なお、欧州指令96/9/ECでは、創作性のないデータベースであっても製作者の投資を保護するため「独自の権利（sui generis right）」を認めている。同権利に対しては、科学の発展を阻害する可能性があるとして、国際科学会議（ICSU）、全米科学アカデミー、日本学術会議等の学術団体が導入反対を表明している。

著作物のデジタル化は著作権法上、複製として扱われる。デジタル方式の複製はコピーによる劣化が生じないため、放置すれば著作権者の権利を大きく侵害するおそれがある。さらにインターネットの登場によりネットワークによる著作物の送信が深刻な問題を引き起こしている。デジタル化やネットワーク化への対応等のため、世界知的所有権機関（World Intellectual Property Organization: WIPO）は議論を重ね、1996年に「著作権に関する世界知的所有権機関条約」及び「実演及びレコードに関する世界知的所有権機関条約」を採択した。両条約では、インターネット上の著作物のインタラクティブ送信やアップロードを対象とする「公衆への伝達権」が創設され、これを受けて日本は1997年の著作権法改正により公衆送信権及び送信可能化権を設け、世界に先駆けて国内法の整備を行った。インターネットに対応する権利が著作権法に設けられたことにより、誰もが著作権者にも侵害者にもなりうる時代が到来したのである。

デジタルデータと著作権侵害については、近年インターネット上の違法アップロード及び違法ダウンロードが問題となっている。著作権者の許諾なしにインターネット上に動画や音楽をアップロードし不特定多数の者がダウンロードできる状態に置くことは、著作権侵害行為であり処罰される。一方で、違法にアップロードされた動画や音楽を個人がダウンロードして楽しむ行為は、著作権法第30条第1項の私的使用目的に該当するとして、長らく著作権侵害行為ではなかった。しかし、氾濫する違法アップロードを踏まえ、2009年著作権法改正において、第

30条第1項第3号により違法アップロードと知りながら動画や音楽を録音・録画する行為が私的使用の対象外となり、著作権侵害行為となった。さらに、2012年改正で第119条第3項が追加され、刑罰が科されることになった(2)。この違法ダウンロードの刑事規制については、対象とする著作物が有償で公衆に提供・提示されているものに限られる。また、違法となる行為が「録画・録音」であるため、動画サイトにアップロードされた動画や音楽をストリーミング再生する行為は対象にならないと考えられている(3)。

●事例研究

■Appleの海賊版電子書籍

2010年12月、日本書籍出版協会、日本雑誌協会、日本電子書籍出版社協会及びデジタルコミック協議会の4団体は、違法な電子書籍の配信に関してAppleに対する抗議声明を公表した。声明は、タブレットやスマートフォン向けのコンテンツ販売サイトであるApp Storeで、日本の作家の作品が違法に配信されていたことを踏まえ、同サービスを運営するAppleに対して削除要請を行ってきたものの、大半の違法配信が継続されていたことから、Appleに重大な責任があると非難し、海賊版に関する情報開示と防止策の策定を求めたものである(4)。関係者によれば、「Apple主導で削除に対応するようになってきている。」(5)とされている。

●海外の状況、技術動向、制度、規制

■Googleブックス検索問題

米国のGoogleのサービスである「Googleブックス」では、大学図書館等と連携し、その蔵書をデジタル化し検索可能にする「Googleブックス図書館プロジェクト」を行っている(6)。これに対して米国作家協会（Authors Guild）等が著作権侵害に当たるとして集団訴訟を提起した。2008年10月に和解案、2009年11月に修正和解案について合意が得られ、Googleの書籍のデジタル化等を可能とする一方、著作権者に対して補償金及び収益の一部を支払うこと等が定められたものの、2011年3月に連邦裁判所で和解案の承認が拒否された。その後、2013年11月の連邦地方裁判所判決では、Googleブックスについて、フェアユースに当たり著作権侵害に該当しないとして、米国作家協会の訴えを棄却したが、同協会が控訴したため、最終的な決着は見ていない。なお、米国出版社協会（AAP）との間では、2012年10月に和解が成立した。

2008年に和解案が公表された際、和解案の効力が米国の訴訟当事者に留まらず、全世界の著作権者に及ぶことが明らかになり大きな問題となった。日本でも著作権・出版者の団体が抗議を行ったが、2009年の修正和解案の段階で、日本やヨーロッパの出版物は対象から除かれた。

(1)　「著作権制度の概要4.著作者の権利（1）著作物」著作権なるほど質問箱ウェブサイト <http://chosakuken.bunka.go.jp/naruhodo/outline/4.1.html>
(2)　この改正をめぐる動きについては次の資料を参照。齋藤千尋「違法ダウンロード刑事規制をめぐる動き―平成24年著作権法改正―」『調査と情報―ISSUE BRIEF―』760号, 2012.10.18. <http://dl.ndl.go.jp/view/download/digidepo_3580528_po_0760.pdf?contentNo=1> 主要国の制度については次の資料を参照。前橋奈保子「インターネット上の著作権侵害に関する各国の法制度」『調査と情報―ISSUE BRIEF―』747号, 2012.4.5. <http://dl.ndl.go.jp/view/download/digidepo_3487281_po_0747.pdf?contentNo=1>
(3)　文化庁「違法ダウンロードの刑事罰化についてのQ&A」2012.7.24. <http://www.bunka.go.jp/chosakuken/download_qa/pdf/dl_qa_ver2.pdf>
(4)　日本書籍出版協会ほか「アップル社「アップストア」におけるデジタル海賊版の問題について」2010.12.14. <http://www.jbpa.or.jp/pdf/documents/applepress1214.pdf>
(5)　日本書籍出版協会「出版物の主に日本国内の海賊版の被害実態について」（第4回文化審議会著作権分科会出版関連小委員会資料1）2013.6.24. 文化庁ウェブサイト <http://www.bunka.go.jp/Chosakuken/singikai/shuppan/h25_04/pdf/shiryo_1.pdf>
(6)　「Googleブックス図書館プロジェクト―世界中の書籍の高性能カタログ―」Googleウェブサイト <http://www.google.co.jp/intl/ja/googlebooks/library.html>

5.2.4　サイバー犯罪とその対策

我が国では、サイバー犯罪に対して不正アクセス禁止法を始めとした法制度を整備し、罰則を設けている。警察庁では、違法情報・有害情報の通報を受け付けるインターネット・ホットラインセンターや、各都道府県警に設置されたサイバー犯罪相談窓口等のサイバー犯罪対策体制（サイバーポリス）においてサイバー犯罪の取締りを行っている。

年々増加するサイバー犯罪に対して、我が国では以下のような法制度を整備し罰則を設けるとともにその取締に当たっている。

表1　サイバー犯罪に関わる主な法律

通称	正式名称	概要
不正アクセス禁止法	「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）	不正アクセス行為、他人の識別符号（ID・パスワード）の不正取得・保管、ID・パスワードの譲渡、フィッシング行為等を禁止。
刑法 （サイバー刑法を含む）	「刑法」（明治40年法律第45号） （「情報処理の高度化等に対処するための刑法等の一部を改正する法律」（平成23年法律第74号））	電磁的公正証書原本不実記録罪、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、電磁的記録毀棄罪、不正指令電磁的記録に関する罪等を規定。
特定電子メール法・特定商取引法	「特定電子メールの送信の適正化等に関する法律」（平成14年法律第26号）・「特定商取引に関する法律」（昭和51年法律第57号）	いわゆる迷惑メールを規制するための法律。
出会い系サイト規制法	「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」（平成15年法律第83号）	出会い系サイトの利用に起因する児童買春その他の犯罪から児童を保護することを目的とした法律。サイト運営者に利用者が児童でないこと等を確認する義務を課している。
児童ポルノ禁止法	「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」（平成11年法律第52号）	児童買春、児童ポルノに係る行為等を処罰するための法律。なお、2014年改正により、児童ポルノの単純所持が禁止され、刑事罰が科されるようになった。
リベンジポルノ防止法	「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」（平成26年法律第126号）	元交際相手等の他人の性的画像を本人の同意なくインターネット上で公開する行為（いわゆる「リベンジポルノ」）に対する罰則を規定。

（出典）各種資料を基に三菱総合研究所作成。

我が国のサイバー犯罪対策として、警察庁から委託されたインターネット協会が運営するインターネット・ホットラインセンターが設置されており、違法情報・有害情報の通報を受け付けるとともに、警察庁を中心に各都道府県警にサイバー犯罪相談窓口等のサイバー犯罪対策体制（サイバーポリス）を置いて対処してきた。さらに、近年のサイバー犯罪の高度化・複雑化に対応するため、捜査員等の増員や、都道府県警察からの派遣要請に機動的に対応できる「機動解析班」を管区警察局・都道府県（方面）情報通信部等の情報技術解析課に設置している。2014年には巧妙化が進む不正プログラム等の高度な技術を要する情報技術の解析やそのために必要となる技術開発を行うため、警察庁情報通信局情報技術解析課に「高度情報技術解析センター」を設置し、犯罪捜査における技術支援体制の中核として各都道府県警を支援している(1)。

加えて捜査員の能力向上のため、2014年4月に警察大学校に「サイバーセキュリティ研究・研修センター」を設置し、サイバー犯罪・サイバー攻撃の取締りに必要な専門的知識・技術に

関する研修を実施している(2)。

捜査手法についても見直しを進めており、全国協働捜査方式（発信元所在地が不明の違法情報について警視庁に設置した情報追跡班が発信元を割り出し、発信元を管轄する都道府県警察がその後の捜査を行う方法）の導入や、サイバー犯罪における捜査特別報奨金制度の活用により警察への情報提供を促すなどを実施している。また、ハッカーからの協力の確保、おとり捜査の積極的活用なども検討されている(3)。

●事例研究

■国際的ボットネットテイクダウン作戦

不正プログラム「Game Over Zeus」が世界中に蔓延し、インターネットバンキングの不正送金事犯に使用されている。Game Over Zeus は感染し乗っ取った多数のコンピュータをネットワーク化（いわゆるボットネット）する。2014年6月、警察庁では、米国連邦捜査局（Federal Bureau of Investigation: FBI）及び欧州刑事警察機構（European Police Office: Europol,「ユーロポール」と読む。）等と連携し、Game Over Zeusのネットワークを崩壊させる（ボットネットのテイクダウン）作戦を実施したことを発表した。(4)

●海外の状況、技術動向、制度、規制

■米国NCFTA

米国のNCFTA（National Cyber-Forensics and Training Alliance）は産業界が直面するサイバー空間の脅威に産学官が共同して対処するため、1997年にFBI、民間企業、学術機関を構成員として設立された非営利団体である。構成員が持つサイバー犯罪に係る情報を集約・分析することで、法執行機関の犯罪捜査を始め民間企業における情報セキュリティ向上等に貢献している。また、トレーニング等を提供することで、産官学の人材育成にも貢献している。(5)

なお、我が国においても、警察庁の総合セキュリティ対策会議の提言に基づき、日本版NCFTAの検討が進められてきた(6)。その結果2014年11月には、産業界、学術機関、法執行機関等それぞれが持つサイバー空間の脅威への対処経験を集約・分析した情報を共有するため日本版NCFTAとして日本サイバー犯罪対策センター（Japan Cybercrime Control Center: JC3）が設立され業務を開始した(7)。

(1)　警察庁情報通信局「警察の情報通信」2014, p.18. <http://www.npa.go.jp/joutuu/pdf/pamphlet.pdf>
(2)　「サイバーセキュリティ研究・研修センター」警察庁ウェブサイト <http://www.npa.go.jp/keidai/keidai.files/cyber.html>
(3)　「サイバー犯罪対処能力の強化等に向けた緊急プログラム―いわゆる遠隔操作ウイルス等による犯行予告事案を受けて―」（平成25 年1月16 日サイバー空間の脅威に対する総合対策委員会決定）警察庁ウェブサイト <http://www.npa.go.jp/cyber/policy/image/program1.pdf>
(4)　「インターネットバンキングに係る不正送金事犯に関連する不正プログラム等の感染端末の特定及びその駆除について―国際的なボットネットのテイクダウン作戦―」警察庁ウェブサイト <http://www.npa.go.jp/cyber/goz/index.html>
(5)　“The NCFTA: Combining Forces to Fight Cyber Crime,”2011.9.16. Federal Bureau of Investigation Website <http://www.fbi.gov/news/stories/2011/september/cyber_091611>;“About the NCFTA.”National Cyber-Forensics and Training Alliance Website <http://www.ncfta.net/about-ncfta.aspx>
(6)　総合セキュリティ対策会議「サイバー空間の脅威に対処するための新たな産学官連携の在り方―日本版NCFTAの創設に向けて―」2014.1. 警察庁ウェブサイト <http://www.npa.go.jp/cyber/csmeeting/h25/pdf/h25_honpen.pdf>
(7)　日本サイバー犯罪対策センター「サイバー犯罪対策新組織「日本サイバー犯罪対策センター（JC3）」の業務開始」2014.11.13. <https://www.jc3.or.jp/media/pdf/pressrelease.pdf>

5.2.5　外国におけるネット検閲

一部の国において、海外のウェブサイトへのアクセスの制限や特定のキーワードに対するブロッキング、サイトへの反政府的な書込みの削除などインターネット上の情報に対する政府機関による検閲行為が行われているとされている。

ネット検閲とは、インターネット上の情報に対して政府機関等の公権力が強制的に表現内容を調査し取り締まることを指す。なお、検閲（Censorship）と監視（Surveillance）は異なる概念であるが、ここでは政府機関によるネット上の監視活動やネット盗聴の事例も含めて紹介する。

日本では憲法第21条第2項において「検閲は、これをしてはならない」と規定しており、ネット検閲も行われない。海外ではネット検閲が行われている事例があり、よく知られている事例として中国政府によるネット検閲がある。中国のネット検閲はインターネットを通じた政治的な結集を防ぐことを目的とし、システムと人による2段階の検閲が行われているとされている。中国公安部は、1998年頃から公安組織の情報化やインターネットの監視網構築を目的とした金盾プロジェクトを開始した。その一環として構築された海外サイトへのアクセスを制限する検閲システムは、「グレートファイアウォール」と呼ばれる(1)。こうした検閲システムでは、人権組織や海外メディア等、特定の海外ウェブサイトへのアクセスを制限したり、検索エンジンやインスタントメッセージ（ネット上でリアルタイムに会話するためのメッセージアプリ）に入力された特定のキーワードに対するフィルタリングが行われたりしている。以前は、外国人等一部のユーザは仮想プライベートネットワーク（VPN）を使うことで、アクセスが許されていないサービスを利用していたが、最近はVPNに対する検閲も強化されており、サービスに接続できない事例が増えているという(2)。こうしたシステムによる検閲に加え、公安部公共信息網絡安全監察局「通称：網絡警察（ネット警察）」に所属する数万人単位のネット検閲官がインターネットを監視することで、反政府的なサイト等の削除を行っているとされている(3)。

なお、中国では自国内のインターネットを自国にふさわしいように統制する「インターネット主権」という考え方を主張しており、この主張のもとネット検閲を正当化している(4)。

また、2009年6月工业和信息化部（工業情報化部）は同年7月以降中国で販売される全てのPCに中国ベンダが開発したフィルタリングソフト「Green Dam Youth Escort」をプリインストールすることを義務付ける計画を公表した(5)。同計画に対して、米国の情報通信技術関連の業界団体が方針の見直しを求める声明を発表したほか(6)、米国国務省も正式に異議を示した(7)。その後、工業情報化部は全PCへのインストールの義務化は撤回したものの、学校やネットカフェなど、公共の場で使用するPCには引き続きインストールを義務付けるとしている(8)。

2013年6月、米ワシントン・ポスト紙及び英ガーディアン紙は、米国国家安全保障局（NSA）がMicrosoft、Yahoo、Google、Facebook、Paltalk、YouTube、Skype、AOL及びAppleらが提供するサービスのサーバにアクセスし、ユーザのデータを収集する「PRISM」という情報収集活動の存在を報じた(9)。これは元NSA及び中央情報局（Central Intelligence Agency: CIA）職員のエドワード・ジョセフ・スノーデン（Edward Joseph Snowden）がリークしたもので、同元職員はスパイ罪等の罪で米当局に刑事訴追され、その後ロシアに亡命している。米政府による情報収集に関しては、軍事目的でNSA主体で運営される通信電波傍受システムのエシュロン（ECHELON）の存在、また

ECHELONのアンテナを設置するなどの参加国・協力国の存在も指摘されている(10)。

●事例研究

■青少年インターネット環境整備法に対する反発

2008年6月に制定され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）では第17条第1項において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。青少年インターネット環境整備法案の検討段階では、インターネット先進ユーザーの会（現:インターネットユーザー協会）が同法案について、健全な情報を発信する個人や、サービスを提供する企業などにまで制限をかけてしまうことは、結果的に国家による検閲につながりかねないとの懸念を示し、法案に反対する声明を公開した。(11)

●海外の状況、技術動向、制度、規制

■Googleの中国市場からの撤退

Googleは2006年にGoogleの中国本土版ドメイン「google.cn」を提供する際、一部の検索結果に自主検閲を付ける条件に同意し、検索エンジンの提供を行ってきた。しかし、中国国内での中国政府によるインターネット上の言論統制の強化や、中国の人権活動家のGmailアカウントに中国国内からと思われる不正アクセスがあったことを受けて、2010年3月、中国本土における検索エンジンサービスの撤退を表明した。ただし、検索エンジンの提供以外の研究開発事業は継続する方針としている。なお、香港及びマカオは前述のグレートファイアウォールの管轄外であるため、中国本土のサービス撤退以後、「google.cn」へのアクセスは香港版ドメイン「google.com.hk」にリダイレクト（転送）される。しかし、香港版でも検索結果が表示されないケースも多く、中国政府が何らかの検閲を行っている可能性が指摘されている。(12)

---

(1)　“How does China censor the internet?” *Economist*, April 21, 2013. <http://www.economist.com/blogs/economist-explains/2013/04/economist-explains-how-china-censors-internet>; “The Great Firewall of China: Background,” June 1, 2011. Torfox Website <http://cs.stanford.edu/people/eroberts/cs201/projects/2010-11/FreedomOfInformationChina/the-great-firewall-of-china-background/index.html>

(2)　“China's ‘Wall’ Hits Business,” *Wall Street Journal*, February 13, 2013. <http://www.wsj.com/articles/SB10001424127887323926104578277511385052752>

(3)　李小牧・蔡成平『微博（ウェイボー）の衝撃:中国を変えた最強メディア』阪急コミュニケーションズ, 2012, p.54.

(4)　「中国が主張する「インターネット主権」は妙案か」『ウォール・ストリート・ジャーナル日本版』2014.6.23. <http://jp.wsj.com/articles/SB10001424052702303319204579642012198975536>

(5)　“China Squeezes PC Makers,” *Wall Street Journal*, June 8, 2009. <http://www.wsj.com/articles/SB124440211524192081>

(6)　“Big Business Groups Complain to China's Premier,” *Wall Street Journal*, June 27, 2009. <http://www.wsj.com/articles/SB124599434995459155>

(7)　The U.S. Department of State, “State Department Daily Press Briefing,” June 22, 2009. IIP Digital Website <http://iipdigital.usembassy.gov/st/english/texttrans/2009/06/20090623115637xjsnommis0.1114923.html#axzz3H2N3NOZ4>

(8)　“Installation of Internet filtering software not compulsory: minister,” August 13, 2009. Xinhuanet Website <http://news.xinhuanet.com/english/2009-08/13/content_11875099.htm>

(9)　“U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program,” *Washington Post*, June 7, 2013. <http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html>; “NSA Prism program taps in to user data of Apple, Google and others,” *Guardian*, June 7, 2013. <http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>

(10)　European Parliament, “Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098(INI)),” July 11, 2001. <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A5-2001-0264+0+DOC+PDF+V0//EN>

(11)「共同声明：私たちは青少年ネット規制法案に反対します」2008.4.22. インターネットユーザー協会ウェブサイト <http://miau.jp/1208861775.phtml>

(12)　山田賢一「米グーグル，中国市場からの“撤退”を表明」『放送研究と調査』60(5), 2010.5, p.88.

5.2.6　インターネット上の違法情報・有害情報

インターネット上の違法・有害情報対策として、警察庁によるサイバーパトロールの実施やインターネット・ホットラインセンターの通報窓口の設置のほか、青少年インターネット環境整備法に基づき、事業者によるフィルタリングの提供が義務化されている。

インターネット上の違法情報は「児童ポルノ画像、わいせつ画像、覚醒剤等規制薬物の販売に関する情報等、インターネット上に掲載すること自体が違法となる情報」と定義され、一方、有害情報は「違法情報には該当しないが、犯罪や事件を誘発するなど公共の安全と秩序の観点から放置することのできない情報」と定義される。(1)

政府では、インターネット上の違法・有害情報対策の枠組みとして、2005年に内閣官房にIT安心会議（インターネット上における違法・有害情報等に関する関係省庁連絡会議）を設置し、各省庁間で連携しつつ、インターネット上の違法・有害情報対策を検討している。同会議の下には政府、事業者、業界団体等、関係セクターを横断的につなぐ違法・有害情報対策官民実務家ラウンドテーブルを設置し、関係者間の情報共有、各業界の自主的な取組を推進している(2)。

具体的な取組として、警察庁では、サイバーパトロールを実施して、違法情報の発信者の取締を行うほか、インターネット利用者から違法・有害情報に関する情報提供を受け付ける窓口として、2006年からインターネット・ホットラインセンター（Internet Hotline Center: IHC）を、運用（民間委託）している。IHCは受理した通報を一定の基準に従って選別し、違法・有害情報については警察庁へ通報する。さらに、違法情報については警察庁を通じプロバイダや電子掲示板の管理者等へ削除依頼を行い、違法・有害情報の一部に関しては直接削除依頼等を行う。

違法情報のうち、名誉毀損、著作権侵害等の他人の権利を侵害する情報に対しては刑事上の手続のほか、民事上の手続として「特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律」（いわゆる「プロバイダ責任制限法」。平成13年法律第137号）に基づき、自己の権利を侵害された者又はその代理人は、プロバイダや掲示板の管理者等に対して、権利侵害情報の送信防止措置（削除）(3)の申出や、損害賠償請求権の行使等の目的で情報の発信者（掲示板の書込みをした者等）の情報の開示を求めることができる（発信者情報開示請求）。

2009年、青少年の権利の擁護に資することを目的に「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）が施行された。同法は、民間事業者に「青少年有害情報」(4)のフィルタリングの提供を義務付け、また保護者の責務として青少年に適切にインターネットを利用させることを規定している(5)。なお、表現の自由に配慮し、同法は青少年有害情報について例示するのみで、具体的な判断基準は民間の自主的取組に委ねている(6)。

政府はフィルタリングの導入促進を図るため、携帯電話事業者へのフィルタリングサービス強化の要請、関係事業者と連携したフィルタリング普及キャンペーン等の施策を実施している。

2013年の内閣府の調査によると、青少年の携帯電話・スマートフォンでのフィルタリングの利用率は55.2%であった。特に、スマートフォンのフィルタリング利用率は47.5%と低い結果となった(7)。スマートフォンのフィルタリングを有効にするには、通信事業者のサービスだけでなく、無線LANやアプリに対応したフィルタリングも行う必要があり注意が必要である。

フィルタリングのような技術的な対策に加え、利用者による自制を促すための国民の情報モラル教育も重視されている。現行の小・中・高等学校の学習指導要領では、子どもたちがインターネット上の違法・有害情報等に適切に対応できるよう、各教科等の指導の中で「情報モラル」を身に付けることが明記されるようになっている(8)。

●事例研究

■インターネット・ホットラインセンター（IHC）

IHCにおける通報受理件数は、センターの運用開始以後増加傾向が続いており、2012年には過去最高の約20万件の通報を受理したが、2013年には約13万件と大きく減少した。スマートフォンアプリの利用やサイトの巧妙化により、違法情報が見つけにくくなった可能性がある(9)。2013年中に受理した情報のうち、IHCの分類によると、違法情報は3万371件、有害情報は3,428件であった。またIHCが削除依頼を行った違法情報1万2796件のうち、1万2341件が削除され（削除率は96.4%）、有害情報は1,262件のうち、964件が削除された（削除率は76.4%）(10)。

●海外の状況、技術動向、制度、規制

■International Association of Internet Hotlines（INHOPE）の活動

1995年から1996年にかけて、欧州諸国でインターネット上の児童性的虐待を防ぐ取組や子どもポルノホットラインの設立等の動きが活発化したことを受け、1999年11月23日、欧州委員会が策定した「より安全なインターネット行動計画（Safer Internet Action Plan）」のもと、インターネット・ホットラインセンターの国際的な連合組織としてINHOPE（International Association of Internet Hotlines）が設置された。加盟団体は45か国51団体であり、日本のIHCの運営母体であるインターネット協会も2007年3月からINHOPEに加盟している(11)。

(1)　警察庁『平成24年版警察白書』2012, p.80. <https://www.npa.go.jp/hakusyo/h24/honbun/pdf/08_dai2sho.pdf>
(2)　「違法・有害情報に対する政府等の取組」内閣官房インターネット上の違法・有害情報対策ウェブサイト <http://www.it-anshin.go.jp/policy/index.html>
(3)　プロバイダや掲示板の管理者等は、送信防止措置の申出のあった情報が、①他人の権利が侵害されていると信じるに足りる相当な理由があったとき、又は②権利を侵害されたとする者から違法情報の削除の申出があったことを発信者に連絡し、7日以内に反論がないとき、には発信者に対して責任を負わず情報を削除することができる。
(4)　青少年インターネット環境整備法は、「インターネットを利用して公衆の閲覧（視聴を含む。以下同じ。）に供されている情報であって青少年の健全な成長を著しく阻害するもの」（第2条第3項）と定義し、「人の性行為又は性器等のわいせつな描写その他の著しく性欲を興奮させ又は刺激する情報」や「殺人、処刑、虐待等の場面の陰惨な描写その他の著しく残虐な内容の情報」等を例示している（第2条第4項各号）。
(5)　なお、「子ども・若者育成支援推進法」（平成21年法律第71号）により、青少年インターネット環境整備法は改正され、平成22年4月1日にインターネット青少年有害情報対策・環境整備推進会議から改組された子ども・若者育成支援推進本部が、「青少年が安全に安心してインターネットを利用できるようにするための施策に関する基本的な計画」を定め、その実施を推進することとされた（第12条）。
(6)　インターネット上の違法・有害情報への対応に関する検討会「インターネット上の違法・有害情報への対応に関する検討会最終取りまとめ―「安心ネットづくり」促進プログラム―」2009.1, pp.10, 12, 17. 総務省ウェブサイト <http://www.soumu.go.jp/menu_news/s-news/2009/pdf/090116_1_bs1-1.pdf>
(7)　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結果（概要）」2014.3, p.10. <http://www8.cao.go.jp/youth/youth-harm/chousa/h25/net-jittai/pdf/kekka_g.pdf>
(8)　「現行学習指導要領・生きる力」文部科学省ウェブサイト <http://www.mext.go.jp/a_menu/shotou/new-cs/youryou/>
(9)　「悪質サイト巧妙に、見つけにくく通報33%減、昨年、警察庁「積極的に教えて」」『日本経済新聞』2014.4.24, 夕刊.
(10)　警察庁「平成25年中の「インターネット・ホットラインセンター」の運用状況等について」2014.4.24, p.1. <https://www.npa.go.jp/cyber/statics/h25/pdf03-2.pdf>
(11)　「海外のホットライン」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/about/foreign.html>

5.3　国際的対策

5.3.1　国際協調

2013年10月、政府の情報セキュリティ政策会議において、国際連携・共助に関する我が国の基本方針及びそれに基づく重点取組分野等を整理した「サイバーセキュリティ国際連携取組方針」が策定されている。また、サイバー犯罪は犯罪行為が国境を越えて影響を及ぼすため、欧州評議会が中心となってサイバー犯罪条約が作成され、当初、日本・米国・欧州の主要30か国が署名した。

2013年10月、政府の情報セキュリティ政策会議は「サイバーセキュリティ国際連携取組方針」を策定し、国際連携・共助に関する我が国の基本方針及びそれに基づく重点取組分野等を整理している(1)。本方針によれば、重点的な取組分野として、①情報共有体制、②サイバー犯罪対策、③サイバー安全保障、④グローバルな浄化活動、⑤啓発活動、⑥研究開発、⑦技術基準策定、⑧国際的な規範作り、などが示されている。

①情報共有体制としては、各国のCSIRT（Computer Security Incident Response Team）、法執行機関、政策担当者、外交担当者、研究者など、それぞれのコミュニティにおける連携が想定されている。例として、CSIRT間の国際連携体制であるFIRST（Forum of Incident Response and Security Teams）（用語集参照）の取組などが挙げられる。

②サイバー犯罪対策としての国際協力の代表的な例は、欧州評議会が中心となって作成され、当初、日本・米国・欧州の主要国30か国が署名した「サイバー犯罪に関する条約」（いわゆる「サイバー犯罪条約」。平成24年条約第7号）である。サイバー犯罪条約は、コンピュータシステムに対する違法なアクセス等の行為の犯罪化、コンピュータデータの迅速な保全等に係る刑事手続、犯罪人の引渡等について規定しており、2012年11月1日から日本国内でも効力が生じている。なお、本条約に対応した国内法の整備の一環として、「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）によって、コンピュータ・ウイルス作成罪の新設等が行われている。

また、警察庁では、G8 ローマ／リヨン・グループ(2)のハイテク犯罪サブグループなどの国際連携に取り組んでいる。

③サイバー安全保障は、次項「5.3.2　サイバー空間における安全保障」で説明する。

④グローバルな浄化活動は、各国におけるサイバー事案の検知、分析や対処体制の構築を国際協調の枠組みとして実施しており、例としてはJPCERTコーディネーションセンター（JPCERT/CC）が行っているアジア・アフリカ諸国等に対するCSIRT構築支援等がある(3)。

⑤啓発活動としては、政府や企業のセキュリティ担当者の意識・能力向上策としてセミナー開催や啓発用素材の提供等を行っている。例としては、内閣サイバーセキュリティセンター（NISC）が中心となり毎年10月に実施する「情報セキュリティ国際キャンペーン」(4)がある。

⑥研究開発については、高度な対策技術について国際連携による研究開発を推進している。例としては、サイバー攻撃の発生を予知するため、サイバー攻撃等に関する情報収集ネットワークを諸外国と連携して構築する総務省の研究開発プロジェクトPRACTICE（Proactive Response Against Cyber-attacks Through International Collaborative Exchange）がある(5)。

⑦技術基準策定、⑧国際的な規範作りはサイバー空間上の各種活動に対して国際的なルール作りを進めていくことを目的とした国際協調活動である。例としては、ISOやITUにおける標準化への貢献を行っている。また、国家の情報通信技術の利用に関する規範づくりを促進するため、国連総会第一委員会（主要議題：軍縮、安全保障）の下に設置された政府専門家会合に参加したことなども挙げられる。

●事例研究

■TSUBAME（アジア・太平洋地域インターネット定点観測可視化プロジェクト）

TSUBAMEは、日本のJPCERT/CCが中心となって実施しているインターネット定点観測可視化プロジェクトである。TSUBAMEにはアジア太平洋地域の23チームが参加しており、各チームに設置されたセンサが検出した悪意のある活動を集約することで、サイバー攻撃への対応や脅威情報の共有・分析を協力して行っている。(6)

■日・ASEAN情報セキュリティ政策会議

2009年から、日本がASEAN諸国と情報セキュリティ分野において連携を強化することを目的として、「日・ASEAN情報セキュリティ政策会議」が開催されている。日本からは内閣官房、総務省、経済産業省の政策統括官・審議官等、ASEAN加盟国からは経済・投資関係省庁及び情報通信関係省庁の次官補・局長・審議官が出席している。2014年10月には東京において第7回会議が開催された。第7回会議では、日・ASEANにおける重要インフラ防護、情報セキュリティ関連の情報共有体制等に関して各国の連携を確認している(7)。

●海外の状況、技術動向、制度、規制

■サイバー空間に関するソウル会議

2013年10月17日から18日にかけて、「サイバー空間に関するソウル会議」が韓国のソウルにおいて開催された。本会議は、2011年にロンドン、2012年にブダペストにおいて開催された会議のフォローアップ会合であり、「オープンで安全なサイバー空間を通じた世界的繁栄」をテーマとして、87か国の政府関係者、国際機関、民間セクター、学者、NGO代表など約1,600名が参加した大規模な会合である。日本からは外務副大臣を筆頭とした代表団が参加した。代表団には内閣官房、外務省、総務省、経済産業省、防衛省及び警察庁が含まれている。(8)

---

(1)　情報セキュリティ政策会議「サイバーセキュリティ国際連携取組方針―j-initiative for Cybersecurity―」2013.10.2. <http://www.nisc.go.jp/active/kihon/pdf/InternationalStrategyonCybersecurityCooperation_j.pdf>
(2)　1978年のG7（当時）のボン・サミットにおいてハイジャック対策や国際テロに関する意見交換を行う場として設置された専門家会合（ローマグループ）と、1995年のハリファックス・サミットで設置されたG8国際組織犯罪上級専門家会合（リヨン・グループ）が、2001年の米国同時多発テロ事件以降開催している合同会合の名称。「国際的な警察活動（国際的連携の強化）」警察庁ウェブサイト <https://www.npa.go.jp/kokusaikyoryoku/kyouka/lyong.htm>
(3)　経済産業省「経済産業省の情報セキュリティに関する国際連携と意識啓発活動等」（第31回情報セキュリティ政策会議参考3）2012.11.1. <http://www.nisc.go.jp/conference/seisaku/dai31/pdf/31shiryous03.pdf>
(4)　「情報セキュリティ国際キャンペーン」内閣サイバーセキュリティセンターウェブサイト <http://www.nisc.go.jp/security-site/campaign/>
(5)　本田知之「総務省における情報セキュリティ政策の最新動向」（沖縄ICTフォーラム2014 in 久米島）2014.7.3, p.11. 日本インターネットプロバイダー協会ウェブサイト <http://www.jaipa.or.jp/event/oki_ict2014/140703_honda.pdf>
(6)　「TSUBAME（インターネット定点観測システム）」2015.2.27. JPCERTコーディネーションセンターウェブサイト <https://www.jpcert.or.jp/tsubame/>
(7)　内閣官房情報セキュリティセンターほか「第7回日・ASEAN情報セキュリティ政策会議の結果」2014.10.8. <http://www.nisc.go.jp/press/pdf/aseanj_meeting20141008.pdf>
(8)　「サイバー空間に関するソウル会議」2013.10.22. 外務省ウェブサイト <http://www.mofa.go.jp/mofaj/gaiko/page18_000084.html>

5.3.2　サイバー空間における安全保障

近年はサイバー攻撃が顕著になり、国家安全保障上の重要課題となっている。2014年3月にサイバー攻撃に対処するため、自衛隊の専門部隊として「サイバー防衛隊」が発足した。また外務省は日米同盟の強化といった観点から日米サイバー対話を開催している。

近年、2007年のエストニアへのサイバー攻撃や、2013年の韓国へのサイバー攻撃などを踏まえ、日本でも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。2013年12月に閣議決定された国家安全保障戦略においても一節を設け、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っている。また、2013年6月に策定された「サイバーセキュリティ戦略」においても、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。

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の実施、サイバー攻撃に関する脅威情報の収集、分析等を一元的に行うものである。また、日米防衛協力のための指針（いわゆる「ガイドライン」。）の改訂に際してサイバー攻撃対策を盛り込む方向で検討を行っている(1)。

そのほか、米国防総省との間では、日米サイバー防衛政策ワーキンググループ（CDPWG）、日米ITフォーラム、日米情報保証実務者定期協議（IAWG）等を開催し連携関係を深めている。

なお、サイバー攻撃の法的位置付けについては国際的にも十分に整理されていない。また、サイバー攻撃が自衛権発動の対象となるか、自衛権発動の第一要件（概論「サイバーセキュリティに関する法律及び制度」注(13)参照）を満たすか、などについても議論がある。サイバー攻撃を受けた際に反撃する能力については「相手方によるサイバー空間の利用を妨げる能力」として、「中期防衛力整備計画（平成26年度～平成30年度）」において検討するものとされている(2)。ただし、専守防衛との関係で、どこまでの反撃が可能かについての結論は出ていない。

警察庁においてもサイバー攻撃・サイバーテロ対策が行われている。警察庁警備局警備企画課にサイバー攻撃分析センターを設置するとともに、13の都道府県警察にサイバー攻撃特別捜査隊を置いてサイバー攻撃関連情報の収集、犯罪の予防、捜査を行っている。

日米同盟の文脈では2011年6月に開催された日米安全保障協議委員会（いわゆる「2+2」。）において、初めてサイバー空間の保護が安全保障上重要な位置を占めることが示され、日米協力を行っていくことが合意されている(3)。これを受けて2012年4月に開催された日米首脳会談の後に発表された日米協力イニシアティブにおいて、両国で「サイバー協力」を行っていくことが合意された(4)。

首脳間合意に基づく、日米サイバー対話が2013年5月と2014年4月に開催された。同会議への日本側参加者は、外務省、国家安全保障局、内閣官房（安全保障・危機管理担当）、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））、内閣情報調査室、警察庁、総務省、経済産業省、防衛省等、また、米国側参加者は国務省、国土安全保障省、司法省、国防総省等であり、ともに幅広い政府関係者が参加している。

外務省では日米二国間協議だけでなく、イギリス、インドとの間でもそれぞれ二国間協議・対話を行うとともにサイバー空間に関するソウル会議（5.3.1　国際協調参照）等の多国間協議を

行っている。

●事例研究

■自衛隊におけるサイバー攻撃対策

統合幕僚監部自衛隊指揮通信システム隊の下に設置されたサイバー防衛隊は防衛省・自衛隊のネットワークの防護を任務としており、約90名の規模で発足した。機能としては、①24時間体制でのネットワーク監視、サイバー攻撃発生時の事案対処、②サイバー攻撃に関する情報収集・分析とその結果の共有、③統合訓練の実施・評価並びに省内機関に対する訓練支援、④マルウェア解析を含むサイバー攻撃・防御手法の調査研究、⑤省内機関に対する技術支援を行っている(5)。

また、サイバー防衛隊以外にも、陸海空自衛隊はそれぞれ、システム防護隊、保全監査隊、システム監査隊として、サイバー防衛を行う専門部隊を有している。

●海外の状況、技術動向、制度、規制

■米国CYBERCOM

2009年6月、ロバート・ゲーツ（Robert Gates）国防長官が、統合戦略軍の下に、サイバー攻撃等に対応するサイバー軍（United States Cyber Command: USCYBERCOM）の設置を命じた(6)。本拠地は米国国家安全保障局（National Security Agency: NSA）の本拠地でもあるメリーランド州のフォート・ミード陸軍基地にあり、2010年5月の活動開始時は1,000名体制で、2014年予算は4億4700万ドルであった。2016年までに6,000名体制への増員を目指している(7)。

■NATOタリン・マニュアル

NATOがエストニアのタリンに設置したサイバー防衛センター（NATO CCDCOE）は「サイバー戦に適用される国際法に関するタリン・マニュアル」（タリン・マニュアル）を2013年にまとめた(8)。タリン・マニュアルで注目されるのは、サイバー攻撃に対しては一定の条件のもとで軍事的対応をとりうるとの見解を示したことである。タリン・マニュアル自体は専門家会合における議論の成果であり、NATOの公式見解ではない点に留意する必要はあるが、今後同種の議論に大きな影響を及ぼすものと予想されている。

---

(1)　「日米防衛協力のための指針の見直しに関する中間報告」2014.10.8. 防衛省ウェブサイト <http://www.mod.go.jp/j/approach/anpo/sisin/houkoku_20141008.html>
(2)　「中期防衛力整備計画（平成26年度～平成30年度）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）<http://www.mod.go.jp/j/approach/agenda/guideline/2014/pdf/chuki_seibi26-30.pdf>
(3)　「＜仮訳＞日米安全保障協議委員会共同発表―より深化し，拡大する日米同盟に向けて：50年間のパートナーシップの基盤の上に―」2011.6.21. 外務省ウェブサイト <http://www.mofa.go.jp/mofaj/area/usa/hosho/pdfs/joint1106_01.pdf>
(4)　「ファクトシート：日米協力イニシアティブ（仮訳）」2012.4.30. 外務省ウェブサイト <http://www.mofa.go.jp/mofaj/kaidan/s_noda/usa_120429/pdfs/Fact_Sheet_jp.pdf>
(5)　第186回国会衆議院安全保障委員会議録第6号　平成26年4月8日　p.19.
(6)　US Department of Defense,“U.S. Cyber Command Fact Sheet,”May 25, 2010. <http://www.defense.gov/home/features/2010/0410_cybersec/docs/CYberFactSheet%20UPDATED%20replaces%20May%2021%20Fact%20Sheet.pdf>
(7)　“The Cyber Domain - Security and Operations.”U.S. Department of Defense Website <http://www.defense.gov/home/features/2013/0713_cyberdomain/>
(8)　“Research: Tallinn Manual.”NATO Cooperative Cyber Defence Centre of Excellence Website <http://www.ccdcoe.org/research.html>

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。