サイバーセキュリティに関する法律及び制度

要　旨

我が国では内閣官房に設置された情報セキュリティセンター（NISC）と関係省庁、特に庶務協力5省庁と呼ばれる警察庁、総務省、外務省、経済産業省、防衛省が中心となってサイバーセキュリティ政策が推進されている。サイバーセキュリティ関連法として、様々な立法措置が講じられてきているが、今後は、2014年に成立したサイバーセキュリティ基本法に基づき、サイバーセキュリティ政策が実施されることになる。情報通信技術は進歩が早いことから、サイバーセキュリティ政策推進体制、法律及び制度等の整備が後手に回りがちで様々な課題が生じている。

本論では、日本のサイバーセキュリティに関する体制、法律及び制度について論じる。

I　政策の推進体制

2005年4月20日、内閣総理大臣決定により内閣官房に内閣官房情報セキュリティセンター（現:内閣サイバーセキュリティセンター（NISC））が設置された。同年5月30日、高度情報通信ネットワーク社会推進戦略本部長決定により、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））の下に内閣官房長官を議長とする情報セキュリティ政策会議が設置された。以降、多少の変更はあるものの、情報セキュリティ政策会議を「わが国の情報セキュリティに関する問題の根幹に関する事項を決定する母体」(1)とし、その下でNISCが関連省庁と連携しながらサイバーセキュリティ問題に対する取組が進められてきた（図1参照）。

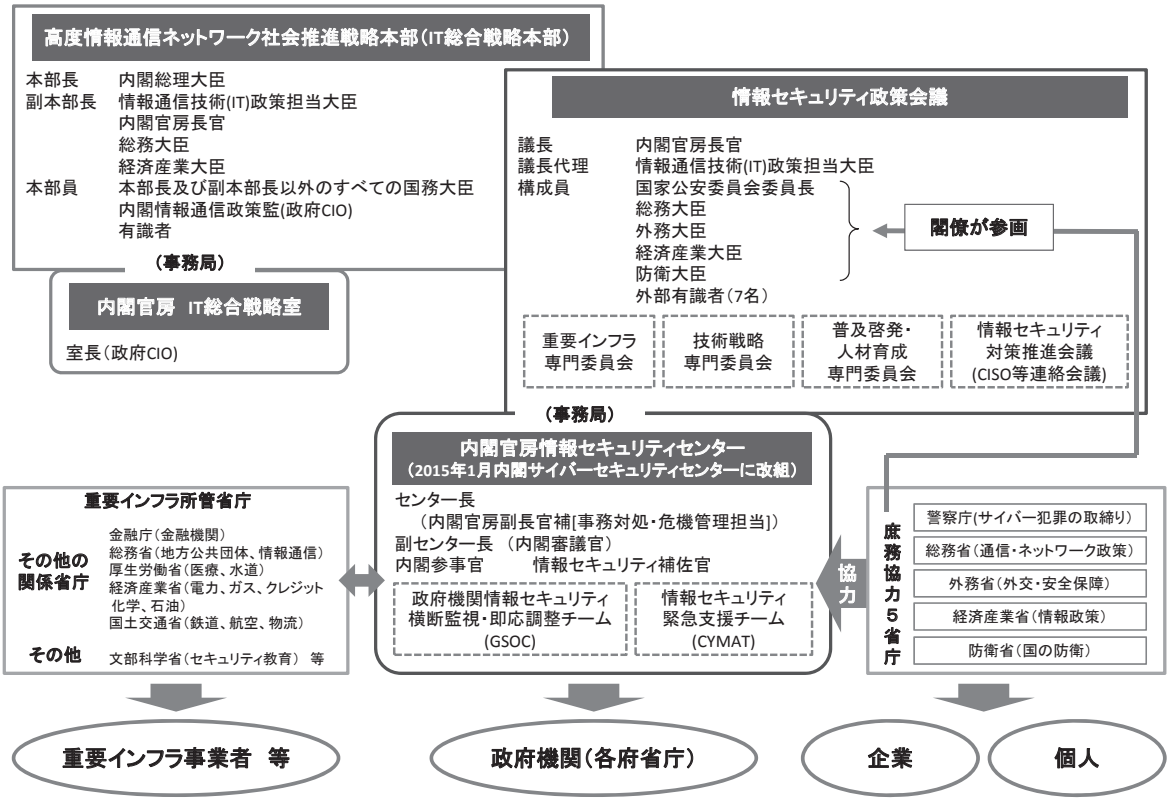
NISC及び情報セキュリティ政策会議では、以下のような政策文書を発行している。

① サイバーセキュリティ戦略：三年間の中期戦略を定めたもの
② サイバーセキュリティ2014：次年度（この場合は2014年度）に関する年次計画
③ サイバーセキュリティ政策に係る年次報告：前年度の年次報告
④ 政府機関の情報セキュリティ対策のための統一規範、政府機関の情報セキュリティ対策のための統一基準：政府機関が実施すべき情報セキュリティ対策について示したもの
⑤ 重要インフラの情報セキュリティ対策に係る第3次行動計画：重要インフラのサイバーセキュリティ確保に向けた行動計画

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

(1)　内閣官房情報セキュリティセンター「情報セキュリティ政策会議の設置について」2005.5.30. <http://www.nisc.go.jp/conference/seisaku/pdf/050530seisaku-press.pdf>

図1　我が国におけるサイバーセキュリティ推進体制



（注）　2015年1月9日のサイバーセキュリティ基本法の全面的施行にともない、内閣に「サイバーセキュリティ戦略本部」が設置され、内閣官房情報セキュリティセンターは「内閣サイバーセキュリティセンター」に改組された。情報セキュリティ政策会議の決定事項及び検討事項等についてはサイバーセキュリティ戦略本部に引き継がれた。

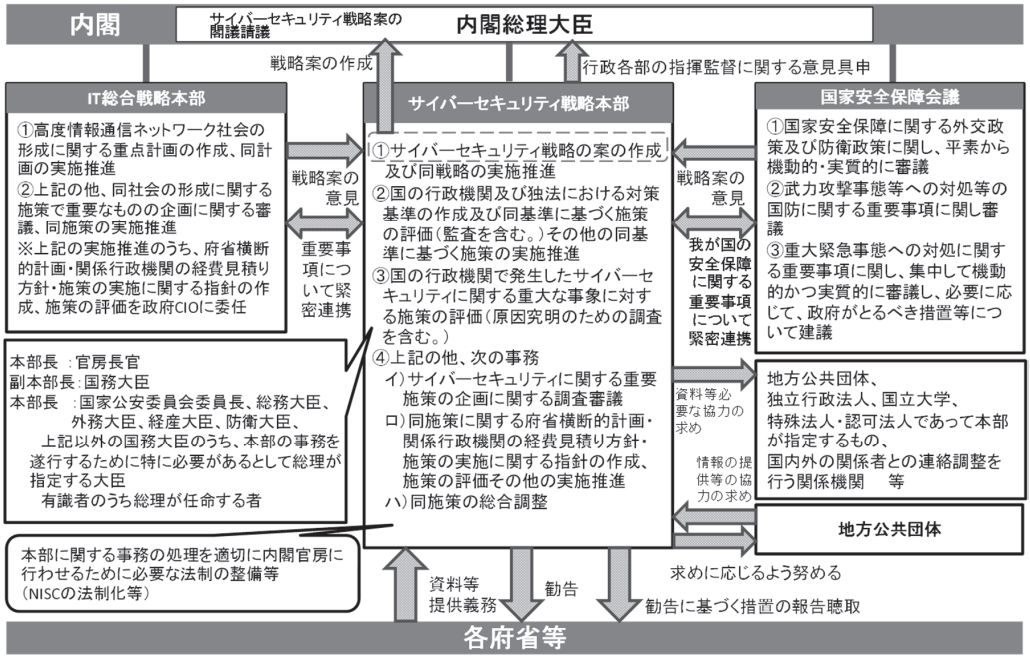
（出典）内閣官房情報セキュリティセンター「わが国のサイバーセキュリティ戦略」2014.10.31, p.4. <http://www.nisc.go.jp/security-site/campaign/ussympo/pdf/keynotelecture.pdf>を基に三菱総合研究所作成。

2014年11月6日に成立した「サイバーセキュリティ基本法」（平成26年法律第104号）により、サイバーセキュリティ推進体制は図2のように変更された。情報セキュリティ政策会議を引き継ぐ組織として「サイバーセキュリティ戦略本部」が設置され、IT総合戦略本部及び国家安全保障会議[(2)]と連携しながら、サイバーセキュリティ戦略等の案の作成を担う。サイバーセキュリティ戦略本部の下でNISCが引き続き事務を担う体制となった。この事務には「行政各部の情報システムに対する不正な活動の監視及び分析」、「重大な事象の原因究明」、「企画及び立案並びに総合調整に関する事務」等が含まれる。

なお、2015年1月9日に施行された「内閣官房組織令及び行政機関職員定員令の一部を改正する政令」（平成26年政令第401号）により、内閣官房情報セキュリティセンターは、内閣サイバーセキュリティセンターに改組された。

(2)　米国の国家安全保障会議（National Security Council: NSC）に倣って、2013年12月に内閣に設置された日本の安全保障に関する重要事項を審議する機関。

図2　我が国におけるサイバーセキュリティ推進体制（2015年1月以降）



（出典）内閣官房情報セキュリティセンター「サイバーセキュリティ基本法案の概要」（第40回情報セキュリティ政策会議資料1-2）2014.7.10. <http://www.nisc.go.jp/conference/seisaku/dai40/pdf/40shiryou0102.pdf>を基に三菱総合研究所作成。

II　法律

我が国のサイバーセキュリティに関する主な法律を表1に示す。

表1　サイバーセキュリティ関連法律

通称	正式名称	概要
IT基本法	「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）	高度情報通信ネットワーク社会の形成に関し、基本理念及び施策の策定に係る基本方針等を定めたもの。
サイバーセキュリティ基本法	「サイバーセキュリティ基本法」（平成26年法律第104号）	サイバーセキュリティに関する施策の推進に当たっての基本理念、関係者の責務、基本的施策、サイバーセキュリティ戦略本部の設置等を定めたもの。
電気通信事業法	「電気通信事業法」（昭和59年法律第86号）	通信事業者における通信の秘密の保護等を定めたもの。
プロバイダ責任制限法	「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」（平成13年法律第137号）	インターネットでのウェブページや電子掲示板などで権利侵害があった場合に、運営管理するプロバイダ等の損害賠償責任の制限と発信者情報の開示を定めたもの。
電子署名法	「電子署名及び認証業務に関する法律」（平成12年法律第102号）	電子署名による電磁的記録の真正な成立の推定等を定めたもの。電子署名に用いることのできる暗号技術を同法の施行規則により定めている。
住民基本台帳法	「住民基本台帳法」（昭和42年法律第81号）	住民に関する諸種の事務処理を統一的に実施するための住民基本台帳制度を定めたもの。
行政手続オンライン化法	「行政手続等における情報通信の技術の利用に関する法」（平成14年法律第151号）	行政機関等に係る申請、届出その他の手続等に関して、電子情報処理組織を使用する方法その他の情報通信の技術を利用する方法等を定めたもの。
e-文書法	「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律」（平成16年法律第149号）	民間事業者等が行う書面の保存等に関し電子情報処理組織を使用する方法その他の情報通信技術を利用する方法等を定めたもの。
電子記録債権法	「電子記録債権法」（平成19年法律第102号）	電子記録債権に係る電子記録を行う電子債権記録機関の業務、監督等について定めたもの。

特定電子メール法	「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）	広告宣伝メールについて、原則としてあらかじめ送信の同意を得た者以外の者への送信禁止、一定の事項に関する表示義務、送信者情報を偽った送信の禁止、送信を拒否した者への送信の禁止等について定めたもの。
特定商取引法	「特定商取引に関する法律」（昭和51年法律第57号）	特定商取引について購入者等の利益を保護し、あわせて商品等の流通及び役務の提供を適正かつ円滑にすることを定めるもので、電子メールによる一方的な商業広告送り付け規制を定めたもの。
特定秘密保護法	「特定秘密の保護に関する法律」（平成25年法律第108号）	我が国の安全保障に関する保護体制について必要な事項を定めるもの。
国家公務員法・地方公務員法	「国家公務員法」（昭和22年法律第120号）、「地方公務員法」（昭和25年法律第261号）	公務員に対して、在職中及び退職後についても職務上知ることのできた秘密について守秘義務を定めたもの。
行政機関個人情報保護法	「行政機関の保有する個人情報の保護に関する法律」（平成15年法律第58号）	行政機関における個人情報の取扱いに関する基本的事項を定めたもの。
個人情報保護法	「個人情報の保護に関する法律」（平成15年法律第57号）	個人情報の保護に関する施策の基本事項及びその保護と利用について定めたもの。
不正競争防止法	「不正競争防止法」（平成5年法律第47号）	事業者の営業秘密の保護のために営業秘密の不正取得・不正使用を禁止することを定めたもの。
著作権法	「著作権法」（昭和45年法律第48号）	著作物・著作者隣接権に関する著作者等の権利保護に関して定めたもの。
刑法（※サイバー刑法）	「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、電磁的記録毀棄罪の処罰等を定めたもの。 2011年（平成23年）の改正で、不正指令電磁的記録に関する罪（コンピュータ・ウイルス作成罪）や電子計算機損壊等業務妨害罪の未遂罪等を新設。
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）	不正アクセス行為や他人の識別符号を不正に取得する行為等の禁止・処罰を定めたもの。 2011年（平成23年）の改正でフィッシング行為等の禁止・処罰を新設。
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）	出会い系サイトの掲示板に児童を相手方とする異性交際を求める書込みをすること（禁止誘引行為）等の禁止・処罰を定めたもの。
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）	児童買春斡旋、勧誘、児童ポルノ所持、提供等の禁止・処罰を定めたもの。 2014年（平成26年）の改正で児童ポルノの単純所持の禁止・処罰を新設。
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不特定多数に公開する行為（いわゆる「リベンジポルノ」）に対する罰則を規定。
会社法	「会社法」（平成17年法律第86号）	業務の適正を確保するため、会社に内部統制システムの確立を義務づけたもの。
金融商品取引法	「金融商品取引法」（昭和23年法律第25号）	財務諸表の信頼性確保の観点から、財務計算に関する書類その他の情報の適正性を確保する体制（内部統制）の確保を上場企業に義務付けたもの。
労働法	「労働基準法」（昭和22年法律第49号） 「労働契約法」（平成19年法律第128号） 「労働者派遣法」（昭和60年法律第88号） ほか	労働基準法では労働契約の不履行について違約金・損害賠償を予定する契約をしてはならないと定めており、また労働契約法では解雇権を濫用してはならないと定めている。 また労働者派遣法では派遣労働者と派遣先企業の間で労働契約を締結しないことを定めている。 企業が情報セキュリティマネジメントを確立する上で労働者管理の観点から考慮する必要のある法律。
民事訴訟法	「民事訴訟法」（平成8年法律第109号）	民事訴訟に関する手続について定めたもの。文書提出命令、準文書など開示について定める。
刑事訴訟法	「刑事訴訟法」（昭和23年法律第131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）	刑事訴訟に関する手続について定めたもの。 2011年（平成23年）の改正で、電気通信回線で接続している記録媒体からの複写、記録命令付差押え、電磁的記録に係る記録媒体の差押えの執行方法、保全要請に関する規定、電磁的記録に係る記録媒体についての差押状の執行を受ける者等に対する協力要請等を新設。

（出典）経済産業省「情報セキュリティ関連法令の要求事項集」2011.4. <http://www.meti.go.jp/policy/netsecurity/docs/secgov/2010_JohoSecurityKanrenHoreiRequirements.pdf>及びその他の資料を基に三菱総合研究所作成。

III　制度・基準

我が国の中央省庁レベルの主な制度等を表2に示す。

表2　サイバーセキュリティ関連制度

制度名称	所管省庁	関連文書	概要
情報通信ネットワーク安全・信頼性対策実施登録制度	総務省	情報通信ネットワーク安全・信頼性基準 情報通信ネットワーク安全・信頼性対策実施登録規程	ネットワークの安全・信頼性対策の実施促進のため、この基準のうち一定の対策が実施されている情報通信ネットワークを登録し公表する制度（1987年開始）。
電気通信事業者における大量通信等への対処と通信の秘密に関するガイドライン	総務省	電気通信事業者における大量通信等への対処と通信の秘密に関するガイドライン	日本インターネットプロバイダー協会、電気通信事業者協会、テレコムサービス協会、日本ケーブルテレビ連盟、日本データ通信協会テレコム・アイザック推進会議の5団体がとりまとめた、電気通信事業法で定められた通信の秘密の保護について違法性がないかどうかを判断するためのガイドライン（2007年策定）。
CRYPTREC （暗号技術検討会）	総務省 経済産業省	電子政府における調達のために参照すべき暗号のリスト （CRYPTREC暗号リスト）	電子政府で利用される暗号技術の評価を行い、電子政府推奨暗号リスト、推奨候補暗号リスト及び運用監視暗号リストを公表する取組（2000年開始）。
FISCガイドライン	金融庁	金融機関等コンピュータシステムの安全対策基準 金融機関等のシステム監査指針	金融情報システムセンター（FISC）が発行する情報システムに係るガイドライン（1985年から順次策定）。金融庁金融検査マニュアルからも参照されている。
ISMS適合性評価制度	経済産業省	JIS Q 27001:2014 （ISO/IEC 27001:2013）	ISMS適合性評価制度は、組織が構築したISMSがJIS Q 27001（ISO/IEC 27001）に適合しているか否かを審査し登録する「認証機関」、審査員の資格を付与する「要員認証機関」、及びこれら各機関がその業務を行う能力を備えているかを認定する「認定機関」からなる総合的な仕組み（2002年開始）。
情報セキュリティ監査制度 （企業台帳）	経済産業省	情報セキュリティ管理基準（平成20年経済産業省告示第246号） 情報セキュリティ監査基準（平成15年経済産業省告示第114号）	企業等組織の情報セキュリティに係るリスクマネジメントが効果的に実施されることを目的に、リスクアセスメントに基づくコントロールの整備、運用が適切に行われていることを、情報セキュリティ監査を行う主体が独立かつ専門的な立場から、国際的にも整合性のとれた基準に従って検証、評価し、保証を与えあるいは助言を行う活動。また、情報セキュリティ監査を担う主体である監査企業等の台帳を整備、公開し、情報セキュリティ監査の普及を図るもの（2003年開始）。
システム監査制度	経済産業省	システム監査基準	組織体の情報システムにまつわるリスクに対するコントロールがリスクアセスメントに基づいて適切に整備・運用されているかを、独立かつ専門的な立場のシステム監査人が検証又は評価することによって、保証を与えあるいは助言を行い、ITガバナンスの実現に寄与することを目的とした制度（1985年開始）。
情報セキュリティ評価認証制度	経済産業省	ISO/IEC 15408（JIS X 5070: 情報技術セキュリティの評価基準）	IT関連製品のセキュリティ機能の適切性･確実性を、セキュリティ評価基準の国際標準であるISO/IEC 15408に基づいて第三者（評価機関）が評価し、その評価結果を認証機関が認証する制度（2001年開始）。
脆弱性関連情報届出制度 （情報セキュリティ早期警戒パートナーシップ）	経済産業省	ソフトウェ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） 情報セキュリティ早期警戒パートナーシップガイドライン	ソフトウェア製品脆弱性関連情報、ウェブアプリケーション脆弱性関連情報の届出を受付、脆弱性関連情報に関して製品開発者への連絡及び公表に係る調整を行う制度（2004年開始）。

（出典）各種資料を基に三菱総合研究所作成。

Ⅳ　課題

我が国のサイバーセキュリティ政策推進体制、法律及び制度に関する代表的な課題について以下にまとめる。

1　対応体制面の課題

我が国のサイバー攻撃に対する対応体制が十分か否かについての議論がある。例えば世界最大規模のサイバー攻撃部隊とされる中国人民解放軍の61398部隊は、正確な数は不明であるが数千人規模(3)、北朝鮮の121局は1,800人規模とする推計もある(4)。これに対して2014年に自衛隊の下に発足したサイバー防衛隊は90人程度とされ(5)、我が国のサイバー攻撃に対する対応体制整備の後れが目立つとの意見もある(6)。

また、サイバーセキュリティ関連予算規模も諸外国に比較して少ない。我が国のサイバーセキュリティ関係の2015年度予算概算要求額は367.8億円であるのに対し(7)、例えば米国の2015会計年度予算教書（概算要求）によれば、約130億ドル（約1兆5000億円）(8)をサイバーセキュリティに支出するとされている(9)。

サイバーセキュリティを支える国産製品の競争力も低い。サイバーセキュリティ対策製品のほとんどは海外製であり、国産技術を用いたものは僅かである(10)。研究開発の側面からも我が国の予算規模の少なさが指摘されている(11)。

2　公共の福祉と権利制限

サイバーセキュリティ対策を理由として、私権の制限がどこまで認められるかについては多くの議論がなされている。例えば以下のような場合に、私権の制限が論点となり得る。

・テロ・犯罪対策を目的とした通信傍受、通信ログの取得、通信遮断等の措置と、通信の秘密の侵害やプライバシー侵害
・スパイ防止やテロ・犯罪対策を目的とした秘密保護（特定秘密保護法、不正競争防止法等）

---

(3)　Mandiant,“APT1 Exposing One of China's Cyber Espionage Units.”<http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf>
(4)　“In North Korea, hackers are a handpicked, pampered elite,”*Reuters*, December 5, 2014. <http://www.reuters.com/article/2014/12/05/us-sony-cybersecurity-northkorea-idUSKCN0JJ08B20141205>
(5)　「サイバー防衛隊発足　防衛システム24時間監視」『日本経済新聞』2014.3.27.
(6)　「日本のサイバー攻撃対処人員確保、人的情報、自衛権…課題山積」『産経ニュース』2015.1.12. <http://www.sankei.com/politics/news/150112/plt1501120024-n1.html>
(7)　内閣官房情報セキュリティセンター「政府の情報セキュリティに関する予算」（第41回情報セキュリティ政策会議資料3）2014.11.25. <http://www.nisc.go.jp/conference/seisaku/dai41/pdf/41shiryou0300.pdf>
(8)　日本円への換算は、日本銀行基準外国為替相場および裁定外国為替相場（2015年1月中において適用）に基づき計算：1ドルについて本邦通貨116円。
(9)　Office of Management and Budget,“Fiscal Year 2015 Budget of the U.S. Government,”2014.3.4. <http://www.whitehouse.gov/sites/default/files/omb/budget/fy2015/assets/budget.pdf>; Richard W. Walker,“Federal IT Spending Slashed In Proposed 2015 Budget,”*InformationWeek*, March 5, 2014. <http://www.informationweek.com/government/cybersecurity/federal-it-spending-slashed-in-proposed-2015-budget/d/d-id/1114126>
(10)　日本ネットワークセキュリティ協会「2013年度情報セキュリティ市場調査報告書」2014.5, p.73. <http://www.jnsa.org/result/2014/surv_mrk/2013_mrk-report_v1.0.pdf>
(11)　情報セキュリティ政策会議「情報セキュリティ研究開発戦略（改訂版）」2014.7.10, p.4. <http://www.nisc.go.jp/active/kihon/pdf/kenkyu2014.pdf>

の施策と、知る権利の侵害
・児童ポルノ等の有害コンテンツの禁止と、表現の自由

また、サイバーセキュリティ対策のために設けられた法制度（コンピュータ・ウイルス作成罪等）が、本来はサイバーセキュリティに資する活動を萎縮させ、ないしは制約する危険が指摘されている(12)。これに関連して、研究者からは、研究の自由をより明確に担保できるような制度の創設を求める意見も出されている。

3　サイバー攻撃への対応

サイバー攻撃の法的位置付けについては十分に整理されていないのが現状である。防衛省における検討によれば「武力攻撃の一環としてサイバー攻撃が行われた場合、自衛権発動の第一要件を満たすことになると考えられる」(13)、とされるが、サイバー攻撃の法的位置付けは国際的にも明確でないため、国際的規範の確立が求められている。また、サイバー攻撃を受けた際に反撃する能力については、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。

4　国境なきサイバー空間の特性に起因する問題

サイバー犯罪は国境を越えて影響を及ぼすため、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証拠保全等に係る刑事手続、犯罪人の引渡し等について規定した「サイバー犯罪に関する条約」（いわゆる「サイバー犯罪条約」(用語集参照)。平成24年条約第7号）(14)が締結されている。これによりサイバー犯罪条約締結国については一定の対応がなされているもの、中国をはじめとしてサイバー犯罪条約に署名していない国も多数あり、またサイバー犯罪を実行する際に踏み台となるコンピュータをサイバー犯罪条約に署名していない国から選ぶことは犯罪者にとって容易であることから、条約自体の実効性には限界がある。

また、クラウドが普及することで、クラウドの持つ潜在的なリスクに無自覚なユーザが増加する可能性がある。例えば、海外のクラウドサービスを利用する場合には、通常はデータの物理的な所在地がわからないが、データの物理的な所在地の法制度等が適用される点（例: 海外法執行機関による情報の差押え等）について十分に理解した上で利用する必要がある。

---

(12)　第177回国会衆議院法務委員会議録第15号 平成23年5月31日 p.6.
(13)「防衛省・自衛隊によるサイバー空間の安定的・効果的な利用に向けて」2012.9. 防衛省・自衛隊ウェブサイト <http://www.mod.go.jp/j/approach/others/security/cyber_security_sisin.html>　自衛隊発動の三要件における第一要件とは「我が国に対する急迫かつ不正の侵害があること」である。なお、同三要件は2014年7月に「自衛の措置としての武力の行使の新三要件」に変更され、第一要件は「我が国に対する武力攻撃が発生したこと、又は我が国と密接な関係にある他国に対する武力攻撃が発生し、これにより我が国の存立が脅かされ、国民の生命、自由及び幸福追求の権利が根底から覆される明白な危険があること」となっている。「国の存立を全うし、国民を守るための切れ目の無い安全保障法制の整備について」（平成26年7月1日閣議決定）<http://www.cas.go.jp/jp/gaiyou/jimu/pdf/anpohosei.pdf>;「国の存立を全うし、国民を守るための切れ目のない安全保障法制の整備について」の一問一答」内閣官房ウェブサイト <http://www.cas.go.jp/jp/gaiyou/jimu/anzenhoshouhousei.html>
(14)「サイバー犯罪に関する条約」外務省ウェブサイト <http://www.mofa.go.jp/mofaj/gaiko/treaty/pdfs/treaty159_4a.pdf>

5　利便性・安全性の向上に伴う新たな問題

情報通信技術の進展に伴う利便性・安全性の向上の副作用として、多くの問題が発生している。具体的には以下のような問題である。

① ビッグデータ／パーソナルデータの利用拡大に伴う、個人情報保護・プライバシー保護に関する問題。

② 生体認証（例：指紋認証）の普及の一方で、生体情報漏えいの危険性が増大する可能性：認証情報が漏えいした場合、パスワードであれば変更すれば良いが、生体認証に用いられる指紋等は変更できないため、問題はより深刻になりうる。

③ 情報通信技術の普及に伴い、ITリテラシーの必ずしも高いとはいえない利用者が増加したことによるサイバー犯罪被害の増加や情報漏えい等が社会問題化している。また、青少年のスマートフォン／インターネット利用の増加に伴う問題（例：リベンジポルノ等）の発生。

6　既存の法制度の限界

情報通信技術の進展に伴い、既存の法制度などが、技術の進展に十分に追随できていないことから問題が発生している。具体的には以下のような問題がある。

① 著作権法：著作権法は最も基本的な権利として複製権を規定しているが、デジタルデータは複製が容易であるという性質を持っており、複製をコントロールすることは現実的に困難となっている。一方で、著作物の再利用やアーカイブを進める際に、著作権法が障害となるような事例も報告されている(15)。

② 製造物責任法：現在はソフトウェア自体に我が国の「製造物責任法」（平成6年法律第85号）は適用されないが、ソフトウェアを組み込んだハードウェアは製造物責任法の対象となる。しかしながら、ハードウェアと抱き合わせで販売されたソフトウェアは製造物責任法の対象となりうるかなど曖昧な領域が存在する。また海外の一部の国（例：ドイツ）ではソフトウェアも製造物責任の対象になるとの解釈があり、世界的な統一見解があるわけではない。

以上のように、サイバーセキュリティに関する体制、法律及び制度に関して多くの課題が明らかになってきている。情報通信技術はほかの技術分野に比較しても進歩が速いことから、体制、法律及び制度の整備がどうしても後手に回る傾向にあることは否めない。今後とも技術の進展に伴う新たな課題の発生について注視していくことが重要である。

執筆：株式会社三菱総合研究所　情報通信政策研究本部　主席研究員　村野（むらの）　正泰（まさやす）
監修：京都産業大学法務研究科　客員教授
慶應義塾大学　名誉教授・弁護士　安冨（やすとみ）　潔（きよし）
奈良先端科学技術大学院大学　教授　山口（やまぐち）　英（すぐる）

(15) 骨董通り法律事務所「米国における著作権関連訴訟文書に係る法的論点整理及び分析等調査報告書」2010.3.1. 文化庁ウェブサイト <http://www.bunka.go.jp/chosakuken/pdf/beikoku_bunseki_houkokusho_itaku.pdf>