Ⅱ－4

情報セキュリティマネジメント

4.1　企業の情報セキュリティに対する取組

情報セキュリティに関わる事件・事故が多発する中、企業においては、情報セキュリティに関する意識や対策などを組織内に徹底するための仕組みである「情報セキュリティガバナンス」の確立に取り組むことが求められている。

(1)　情報セキュリティガバナンスとは

情報セキュリティに関わる事件や事故が多発し、その対策が急がれる一方で、多くの企業では情報セキュリティ対策は利益に直結しない「コスト」として扱われ、その重要性が十分に理解されていない状況にある。しかし、情報資産の効率的・効果的利活用が企業活動の成否を決める現代において、経営者は、情報の管理とリスク管理の一環としての情報セキュリティ対策が経営管理上の重要な要素であるとともに、真剣に取り組むべき経営課題でもあることを認識する必要がある。また、企業が取り扱う情報の中には法令や契約で利用が制限されているものが含まれるなど、情報の取扱自体にリスクが伴うケースがあるだけでなく、例えば、情報流出やシステム障害等の情報セキュリティ事故が発生した場合に企業が事故に適法な範囲で対処したとしても、顧客や取引先などの利害関係者から十分には理解されず、さらなる透明性や事業継続性の確保を求められる可能性もある。このような現状を踏まえ、経営者は、特に情報資産に係るリスク管理を目的に、情報セキュリティに関する意識や取組などを組織内に徹底するための仕組みである「情報セキュリティガバナンス」を確立しなければならない(1)。なお、我が国では、経済産業省設置の「企業における情報セキュリティガバナンスのあり方に関する研究会」による2005年3月の報告書が「情報セキュリティガバナンス」を「コーポレート・ガバナンスと、それを支えるメカニズムである内部統制の仕組みを、情報セキュリティの観点から企業内に構築・運用すること」(2)と定義している。

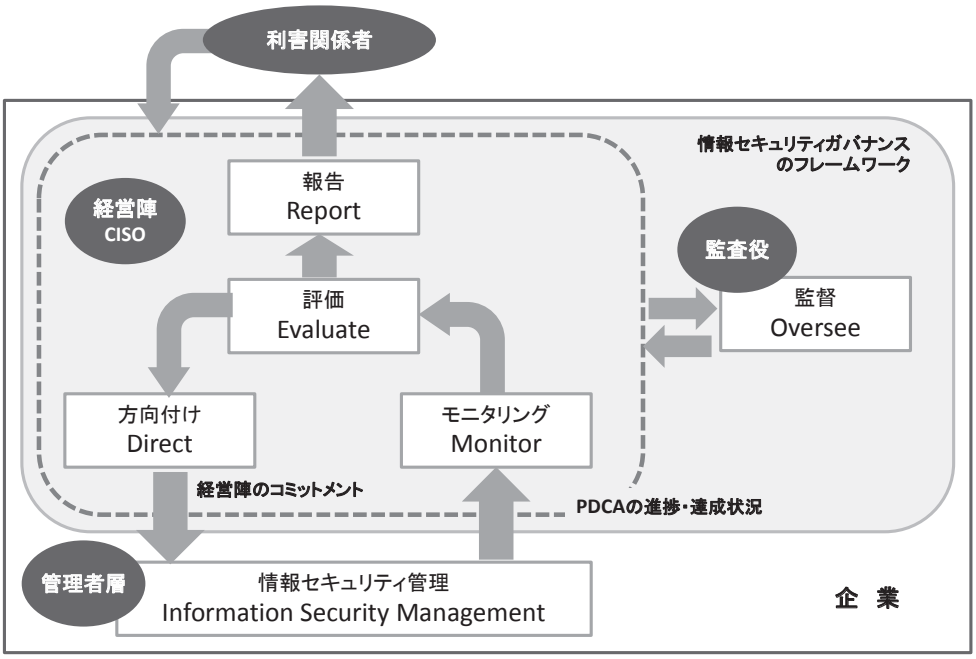
(2)　情報セキュリティガバナンス導入ガイダンス

このような中、経済産業省は、企業における情報セキュリティ対策を、従来の対症療法的なアプローチではなく、「企業価値を高めるための投資対象として位置付けるアプローチの重要性・優位性を示す」(3)ため、2004年度に「企業における情報セキュリティガバナンスのあり方に関する研究会」を開催したほか、2005年度と2006年度に情報セキュリティガバナンスの確立を実現するためのツールとして、「情報セキュリティ対策ベンチマーク」、「情報セキュリティ報告書モデル」、「事業継続計画策定ガイドライン」を開発・公開している。これらの取組を踏まえ、2009年6月には、情報セキュリティマネジメントシステム（Information Security Management System: ISMS）の国際標準ISO/IEC 27001:2005の中の「Management Commitment（経営陣のコミットメント）」に係る経営陣の行動指針や必要な仕組みについて明確化し、ISO/IEC 27001:2005を補完するものとして「情報セキュリティガバナンス導入ガイダンス」を公開している(4)。同ガイダンスでは、経営層と管理者層・従業員層との間でリスクや対策への共通認識が不足していることが原因で、組織全体に最適化された構築や運用がなされていないという問題に対し、経営陣が取り組むべき行動指針を示している。具体的には、情報セキュリティガバナンスのフレームワークは、図1に示すように、経営陣やCISO（用語集参照）（CIO、CSO等が兼ねる場合もあ

る）が「経営戦略やリスク管理の観点から行う「方向付け（Direct）」、ガバナンス活動の状況を指標に基づき可視化する「モニタリング（Monitor）」や結果を判断する「評価（Evaluate）」、これらのプロセスが機能していることを確認する「監督（Oversee）」、結果を利害関係者等に提示する「報告（Report）」の5つの活動から構成される」[5]とされている。

さらに2011年3月には「情報セキュリティガバナンス導入ガイダンス補足編」[6]を公表し、企業グループやサプライチェーン等の組織横断的なグループにおける実効的なセキュリティガバナンスのモデルを示している。

図1　情報セキュリティガバナンスのフレームワーク



（出典）経済産業省「情報セキュリティガバナンス導入ガイダンス」2009.6, p.4. <http://www.meti.go.jp/policy/netsecurity/downloadfiles/securty_gov_guidelines.pdf>を基に三菱総合研究所作成。

2013年4月、組織における情報セキュリティガバナンスの概念や原則、活動に関するガイダンスとして国際標準ISO/IEC 27014:2013が正式に発行され、今後はJIS（日本工業規格）化される予定である[7]。

(3)　中小企業の情報セキュリティ対策の推進

大企業においてはある程度コストをかけて、情報セキュリティ対策を実施することができるが、中小企業において、大企業と同等レベルの対策を実施することは現実的でない。一方で、中小企業の情報化は確実に進んでおり、国内の企業の大部分を占める中小企業において、対策を推進することは非常に重要な課題である。経済産業省所管の情報処理推進機構（IPA）が2009年に中小企業66社に対して行った調査[8]によれば、「情報セキュリティ対策の内容を明確にしているか」との問いに対し、「実施していない」と回答した企業は38社（約58%）に及んでいる。これは、セキュリティに対する認識が不十分であることもあるが、そもそも中小企業は、大企業に比べ、セキュリティにコストをかけることに対するインセンティブが少ないという側面もある。しかし、その一方で個々の取引先から異なる情報セキュリティ対策を求められることもあり、中小企業にとっては大きな負担となりかねない状況になっている。また、同調査に

よれば、ウイルス感染を始めとする何らかの外部からのサイバー攻撃の被害に遭ったことがあると回答したのは66社中48社（約73%）に及んでいる。この結果からも明らかなように、中小企業であっても、セキュリティ対策を疎かにはできない状況にある。

このような中、IPAは2007年から「中小企業の情報セキュリティ対策に関する研究会」を設置して実態に即した中小企業の情報セキュリティ対策の検討を行い、その成果として「中小企業における組織的な情報セキュリティ対策ガイドライン」[9]を公開している。中小企業はそれぞれの企業ごとに規模も業種も異なるため、一律な基準を設けることは難しいが、このガイドラインでは中小企業が共通して実施すべき対策と企業ごとにそれぞれの特徴を考慮して実施すべき対策の2つに分けて説明している。また、IPAは2012年度から商工会議所等と連携して、中小企業の経営者やセキュリティ担当者などを対象に、情報セキュリティに関する管理面・技術面からの対策についてセミナーを行っている[10]。

一方、経済産業省は、日本商工会議所や全国商工会連合会、ITコーディネータ協会の協力の下、日本ネットワークセキュリティ協会（JNSA）に委託して、中小企業の経営者を対象に、情報セキュリティ対策に係る意識の向上を目的とした「中小企業情報セキュリティ対策促進事業」を2008年度から実施している[11]。事業の一環としてJNSAでは、ウェブサイトを通じて中小企業向けの情報セキュリティ対策のための情報提供を行っているほか、2008年度から「中小企業向け指導者育成セミナー」を各地で開催している[12]。

総務省では、各地で情報セキュリティセミナーを開催する一方で、2013年には、省内に設置した「情報セキュリティアドバイザリーボード」からの提言[13]を受け、中小企業の情報セキュリティ対策の底上げを目的に、中小企業の情報セキュリティ投資促進のためのインセンティブを検討するとともに、システムの共同利用など、全体として低コストの情報セキュリティ対策の実現に向けた対策を推進していく方針を打ち出している[14]。

●事例研究

■情報セキュリティガバナンス協議会

2012年5月に、企業や組織が適切な情報セキュリティガバナンスを確立することを促進する目的で「情報セキュリティガバナンス協議会（ISGA）」[15]が設立された。ISGAでは、会員企業限定の意見交換によるベストプラクティスの共有やセミナーなどを通じた情報リスク管理に関する知見の共有、ウェブサイトや冊子、セミナーなどを通じた一般企業向けの情報発信による情報セキュリティガバナンスに関する普及啓発、情報セキュリティガバナンスに関する基準やガイドライン等の策定や改訂、関連コンテンツの整備などを行っている。また、情報漏えいや喪失、情報システムの停止、ネットワークの途絶などの問題によってビジネス上の問題が発生するリスク、いわゆる「情報リスク」に関する経営陣の正しい理解を促すことを目的に、「情報リスクの見える化」にも取り組んでいる。

●海外の状況、技術動向、制度、規制

■米国中小企業庁、連邦通信委員会の取組

米国では中小企業庁（The U.S. Small Business Administration: SBA）がサイバーセキュリティに関する助言集（Tips）[16]を公開している。ただし、独自に作成したものではなく、連邦通信委員会（Federal Communications Commission: FCC）が作成した中小企業向けTips[17]に基づいている。FCC

は米国の放送通信に関する規制監督を行う独立行政機関であるが、その業務の一環として消費者や中小企業の教育を行っている。一方、FCCでは2012年に中小企業が情報セキュリティ向上のための計画を作成するためのガイドラインである「Cyber Security Planning Guide」(18)、及び同ガイドラインに基づき企業ごとにカスタマイズした計画をオンラインで作成できるサービス「FCC Small Biz Cyber Planner 2.0」(19)を提供している。

(1)　経済産業省「情報セキュリティガバナンス導入ガイダンス」2009.6. <http://www.meti.go.jp/policy/netsecurity/downloadfiles/securty_gov_guidelines.pdf>
(2)　「企業における情報セキュリティガバナンスのあり方に関する研究会―報告書―」2005.3, p.9. 経済産業省ウェブサイト <http://www.meti.go.jp/report/downloadfiles/g50331d00j.pdf>
(3)　経済産業省　前掲注(1), はじめに
(4)　同上
(5)　同上, pp.3-4, 6.
(6)　三菱総合研究所「情報セキュリティガバナンス導入ガイダンス 補足編―企業グループにおける情報セキュリティガバナンスモデル―」2011.3. 経済産業省ウェブサイト <http://www.meti.go.jp/policy/netsecurity/docs/secgov/2010_IoformationSecurityGovernanceModel.pdf>
(7)　「2013年4月30日「情報セキュリティガバナンス」の国際標準（ISO/IEC 27014:2013）が正式発行されました。」2013.4.30. 情報セキュリティガバナンス協議会ウェブサイト <http://isga.jp/news/news_130430.html>
(8)　情報処理推進機構セキュリティセンター「中小企業における情報セキュリティ対策の実施状況等調査―調査報告書―」2009.10, pp.2, 13, 15. <http://www.ipa.go.jp/files/000014083.pdf>
(9)　情報処理推進機構「中小企業における組織的な情報セキュリティ対策ガイドライン」2009.3. <https://www.ipa.go.jp/files/000014950.pdf>
(10)「IPA情報セキュリティセミナー」情報処理推進機構ウェブサイト <http://www.ipa.go.jp/security/seminar/isec-semi/>
(11)「中小企業情報セキュリティ対策促進事業とは？」2009.3. 日本ネットワークセキュリティ協会ウェブサイト <http://www.jnsa.org/ikusei/sokusin.html>
(12)「情報セキュリティ対策 中小企業向け指導者育成セミナー―最新動向の理解とグループ討議による実践型研修―」日本ネットワークセキュリティ協会ウェブサイト <http://www.jnsa.org/ikusei/seminar/2014/seminar.html>
(13)　情報セキュリティアドバイザリーボード「総務省における情報セキュリティ政策の推進に関する提言」2013.4.5. 総務省ウェブサイト <http://www.soumu.go.jp/main_content/000217000.pdf>
(14)　総務省編「第1部第3章第2節情報セキュリティと安心・安全な利用」『平成25年版情報通信白書―ICT白書―』日経印刷, 2013, p.301. <http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h25/pdf/25honpen.pdf>
(15)「協議会について」情報セキュリティガバナンス協議会ウェブサイト <http://isga.jp/about/index.html>
(16)　“9 Cyber Security Tips for Small Business Owners,”October 17, 2013. The U.S. Small Business Administration Website <http://www.sba.gov/blogs/9-cyber-security-tips-small-business-owners>
(17)　Federal Communications Commission,“Ten Cybersecurity Tips for Small Businesses,”2012. <http://transition.fcc.gov/Daily_Releases/Daily_Business/2012/db1018/DOC-306595A1.pdf>
(18)　Federal Communications Commission, *Cyber Security Planning Guide*, Penny Hill Press, 2012.
(19)　Federal Communications Commission,“FCC Small Biz Cyber Planner 2.0,”October 2012. <http://www.fcc.gov/cyberplanner>

4.2　情報セキュリティマネジメントシステム

企業や行政機関などの組織において、情報セキュリティを管理する（マネジメントする）ための枠組みとして、情報セキュリティを体系的にとらえたのが情報セキュリティマネジメントシステム（Information Security Management System: ISMS）である。日本では認証基準JIS Q 27001:2014（ISO/IEC 27001:2013）に基づいた適合性評価制度が運用されている。

企業や行政機関などの組織において、情報の機密性（Confidentiality）、完全性（Integrity）、可用性（Availability）（以上の三要素をCIAと呼ぶ）を維持・管理する、つまり情報セキュリティを管理する（マネジメントする）ための枠組みとして、情報セキュリティを体系的にとらえたのが情報セキュリティマネジメントシステム（Information Security Management System: ISMS）である。ISMSとは、情報セキュリティの確立、実施、維持、継続的改善によって、その組織の目的を達成するための、一連の要素（組織の構造、役割及び責任、計画、運用など）のことであり、組織的、人的、物理的、運用的、技術的な対策を含む、経営者を頂点とした組織的な取組である（概論「情報セキュリティマネジメント」を参照）。(1)

ただし、ISMSは組織のセキュリティ水準を保証するものではない。ISMSとは情報セキュリティに関する外部環境・内部環境の変化に対して、組織として絶えず見直しと改善を行う枠組みである。

ISMSに関しては現在、組織がISMSを構築するための要求事項をまとめた国際規格「ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems - Requirements」がある。日本ではISO/IEC 27001:2013をJIS規格化した「JIS Q 27001:2014 情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－要求事項」に基づいて、「ISMS適合性評価制度」が運用されている。同制度においては、日本情報経済社会推進協会（JIPDEC）の情報マネジメントシステム推進センターが認定機関となっている(2)。ISMSでは、JIPDECが取得組織の評価を行うのではなく、JIPDECが認定したISMS認証機関が適合性を評価し認証を行う。日本では同制度に基づくISMS認証機関として26の機関が登録されている（2015年1月26日時点）(3)。

なお、同制度は、国が決めて運用している制度ではないため、厳密には公的な制度ではなく、民間の第三者評価制度である(4)。日本におけるISMS認証取得組織は、2014年12月時点で約4,500組織となっている(5)。ISMS認証取得組織の増加にあわせ、国や自治体の入札において、ISMS認証を取得していることが資格条件とされるケースが増えてきている(6)。ただし、組織は独自の方式でISMSを構築することは可能であるため、認証の有無をもってISMSへの適合・不適合を判断することはできない点に留意が必要である。

また、国際標準化機構（ISO）が2013年に実施した調査によれば、全世界では22,293組織がISMS認証を取得している。対前年比では14%の伸びを示しており、ISOがもつ7つのマネジメントシステム認証制度の全体の伸び率の平均値4%を大きく上回っている。認証取得組織数の上位3か国は日本、インド、英国となるが、増加数ではイタリア、インド、英国の順であった。(7)

●事例研究

■ 国内における情勢

日本では、情報処理サービス業のコンピュータシステムが十分な安全対策を実施しているかを認定する制度として、1981年に「情報システム安全対策実施事業所認定制度」（いわゆる「安対制度」。昭和56年通商産業省告示第342号）が導入されたが、安対制度では情報システムの物理的対策に重点が置かれていたのに対し、技術的対策や人的セキュリティ対策を含む組織全体のマネジメントを確立する必要が出てきたことから、安対制度は2001年に廃止された。安対制度の廃止に伴い、時代のニーズに合わせた新しい制度として、ISMS適合性評価制度が創設され、2002年4月から本格運用を開始した。認定機関はJIPDECの情報マネジメントシステム推進センターである。(8)

●海外の状況、技術動向、制度、規制

■ISO/IEC 27001:2013

ISMSに関して、ISOと国際電気標準会議（IEC）が共同で策定した情報セキュリティ規格群としてISO/IEC 27000ファミリー（主要事項 1.1「情報セキュリティの基礎」を参照）がある。このうち、組織のISMSを認証するための要求事項を定めたのが、「ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems – Requirements」である。

ISO/IEC 27001:2013においては、「供給者関係」という管理策の大項目が新たに追加された。これは旧版（ISO/IEC 27001:2005）の「第三者との契約におけるセキュリティ」や「第三者が提供するサービスの管理」等を含む管理策に加え、新たに外部委託やサプライチェーン（用語集参照）等、外部の製品及びサービスの調達・利用に関する管理策が追加されたものである。新版で追加された具体的な管理策の一つとして「ICTサプライチェーン」がある。この管理策では供給者関係において、供給者との合意にはICTサービスの製品のサプライチェーンに関する情報セキュリティリスクに対処するための要求事項を含めることが推奨されている。(9)

---

(1) 「情報セキュリティマネジメントとPDCAサイクル」情報処理推進機構ウェブサイト <http://www.ipa.go.jp/security/manager/protect/pdca/>
(2) 「情報セキュリティマネジメントシステム（ISMS）適合性評価制度の概要」2014.4.14, 日本情報経済社会推進協会ウェブサイト <http://www.isms.jipdec.or.jp/about/>
(3) 「ISMS認証機関一覧」2015.1.26. 日本情報経済社会推進協会ウェブサイト <http://www.isms.jipdec.or.jp/lst/isr/>
(4) 「FAQ1：制度一般（ISMS）」2014.2.20. 日本情報経済社会推進協会ウェブサイト <http://www.isms.jipdec.or.jp/faq/faq1.html>
(5) 「認証取得組織数推移、認証機関別・県別認証取得組織数」2014.12.25. 日本情報経済社会推進協会ウェブサイト <http://www.isms.jipdec.or.jp/lst/ind/suii.html>
(6) 前掲注(4)
(7) International Organization for Standardization,“The ISO Survey of Management System Standard Certifications – 2013: Executive summary.”<http://www.iso.org/iso/iso_survey_executive-summary.pdf?v2013>
(8) 前掲注(2)
(9) 中尾康二「ISO/IEC 27001&27002の改版の概要と最新情報」pp.113-116. 日本ネットワークセキュリティ協会ウェブサイト <http://www.jnsa.org/seminar/nsf/2014kansai/data/1_nakao.pdf>

4.3　事故前提のセキュリティ対応体制

企業や組織は情報セキュリティ事故が起こることを前提としたセキュリティ体制として組織内部にSOC（Security Operation Center）やCSIRT（Computer Security Incident Response Team）等の対応体制を設置することが求められている。また、CSIRTの国内外提携によるインシデント情報の収集・分析を通じたインシデント対応の高度化が重要になっている。日本では参加組織が増えているもののまだ十分には広まっていない。

警察庁が発表した2013年の不正アクセス行為の発生状況によれば、不正アクセス行為の認知件数は前年比1,700件増の2,951件となっている(1)。また、手口の巧妙化も進んでおり(2)、企業や組織は「100%完全に防ぐことはできない」という事故前提の考えに基づいたセキュリティ対応体制を設置する必要に迫られている。そのような対応体制の中核となるのが、コンピュータセキュリティインシデント（サイバー攻撃等のITシステムの正常な運用や利用の脅威となる事象、以下「インシデント」という。）の発生を速やかに検知するための監視を行うSOC（Security Operation Center, 用語集参照）や、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）である。

CSIRTに関しては、2013年春に各府省庁への設置が完了し(3)、内閣サイバーセキュリティセンター（NISC）が、日本政府のCSIRTとして、各府省庁のCSIRT間の調整役を担っている。また、民間の企業や組織にも政府からCSIRT設置が呼びかけられている(4)。

CSIRTは単に発生したインシデントに対して事後対応を行うだけではなく、使用しているソフトウェアやハードウェアなどの脆弱性対応（修正プログラム「パッチ」の適用など）及び利用者に対する普及啓発や注意喚起などの事前の対応も行う。このような事前と事後の両面から包括的な対策を行う「インシデントマネジメント」の中核を担うのがCSIRTである。

さらにCSIRTは、自組織に限らず、世の中で発生している様々なインシデントに関する情報を収集・分析することで自組織の対処能力を向上させるために、CSIRTのコミュニティに参加して、他のCSIRTと信頼に基づいた情報交換を行い、必要に応じて連携してインシデントに対応する。このような組織間の情報交換の窓口としてCSIRTが国際的に広く認知されている(5)。CSIRTのコミュニティとしては、国際的にはFIRST（Forum of Incident Response and Security Teams）、日本国内では日本シーサート協議会がある。

一方、日本最初のCSIRTとして当時の通商産業省（現：経済産業省）の支援で1996年に正式に発足したJPCERTコーディネーションセンター（JPCERT/CC）は、民間の国際的なCSIRT連携の国内窓口として機能している。例えば、日本国内の企業や組織を騙る偽サイト（フィッシングサイト）が海外で立ち上げられている場合、当該企業・組織からの申告に基づき、偽サイトが設置されている国や地域の国際連携窓口となっているCSIRTに連絡し、対応を促している。また逆に、海外の企業や組織に対して日本国内から不審なアクセスが行われている場合、海外からの問合せに応じて、国内の該当する組織やインターネットサービスプロバイダなどに連絡を行い、事実関係の確認と必要に応じた対応を依頼するなどしている。(6)

なお、フィッシングに関しては、JPCERT/CCが事務局を務めるフィッシング対策協議会が情報収集・提供、注意喚起等の活動を行っている。

●事例研究

■民間企業におけるCSIRTの設置

国内では、政府から各企業や組織にCSIRTの設置が呼びかけられていることもあり(7)、CSIRTを設置する民間企業や組織が増えている。しかし、IPAの調査によればCSIRTを設置している企業は2014年時点で10.8%にとどまっており(8)、十分に普及しているとはいえない。一方、国内のCSIRTのコミュニティとして2007年に発足した日本シーサート協議会の加盟チーム数は2015年2月1日時点で71チームに及び、その半数以上がこの2年間に加盟したチームであることはCSIRT設置が急速に進んでいることを示している(9)。日本シーサート協議会では、参加するCSIRTが収集した脅威情報、脆弱性情報等を共有し、インシデント対応における共通の問題に連携して取り組む等の活動が行われている。

また、近年では組織のCSIRTの運用を支援するツールとして、収集したログ情報に基づいて、異常があった場合に管理者に通知したり、対策方法を知らせたりするSIEM（Security Information and Event Management,「シーム」と読む。）を活用した製品やサービスも多く提供されている。

●海外の状況、技術動向、制度、規制

■CSIRTの国際的なコミュニティ

1988年に世界最初のCSIRTとして米国でCERT/CC が設立された後、1990年には欧米のCSIRTを中心にCSIRTの国際コミュニティFIRST（Forum for Incident Response and Security Teams）が発足した。2014年12月時点で、全世界67の国や地域から309のチームが加盟しており、日本からはNISCやJPCERT/CCを始め、23組織が加盟している(10)。また、アジア太平洋地域の、主に国際連携を担うCSIRTからなるコミュニティAPCERT（Asia Pacific Computer Emergency Response Team）が2003年に発足し、JPCERT/CCが事務局及び議長を務めている。

JPCERT/CCでは各国のCSIRTと協力し、ウイルスの感染活動等のセキュリティ上の脅威となるインターネット上のトラフィックを観測するセンサ網（インターネット定点観測システム）を整備するTSUBAMEプロジェクトを運用しており、観測情報の分析に基づき、インシデント対応や注意喚起などを実施している(11)。

---

(1)　警察庁「平成25年中の不正アクセス行為の発生状況等の公表について」2014.3.27, p.1. <https://www.npa.go.jp/cyber/statics/h25/pdf040.pdf>
(2)　警察庁「第2章　サイバー攻撃情勢」『焦点』283号, 2014.3, p.10. <https://www.npa.go.jp/archive/keibi/syouten/syouten283/pdf/all.pdf>
(3)　内閣官房情報セキュリティセンター「第1回各府省庁PoC会合の開催について」2013.4.10. <http://www.nisc.go.jp/press/pdf/01poc.pdf>
(4)　情報セキュリティ対策推進会議官民連携の強化のための分科会「情報セキュリティ対策に関する官民連携の在り方について」2012.1.19, p.8. <http://www.nisc.go.jp/conference/suishin/ciso/dai4/pdf/1-1.pdf>
(5)　JPCERTコーディネーションセンター「CSIRTガイド」2008.6.24, pp.12-13. <https://www.jpcert.or.jp/csirt_material/files/guide_ver1.0.pdf>
(6)　「JPCERT/CC事業概要」2012.10.25. 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/about/05.html>
(7)　情報セキュリティ対策推進会議官民連携の強化のための分科会　前掲注(4)
(8)　情報処理推進機構「2014年度情報セキュリティ事象被害状況調査―報告書―」2015.1, p.28. <https://www.ipa.go.jp/files/000043418.pdf>
(9)　「会員（チーム）情報」2015.2.1. 日本シーサート協議会ウェブサイト <http://www.nca.gr.jp/member/>
(10)　“FIRST Members.”Forum of Incident Response and Security Teams Website <http://www.first.org/members>
(11)　「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/>

4.4　災害とセキュリティ対策

企業活動の情報システムへの依存度が高まる中、企業は「事業継続計画」（BCP）を、自然災害への対策のみならず、情報セキュリティ対策を含めた形で見直す必要に迫られている。

様々な自然災害が多い日本において、企業は、自然災害などの緊急時に備えた事業継続計画（Business Continuity Plan: BCP）を策定することが求められている。ここで「事業継続計画」とは、「災害時に特定された重要業務が中断しないこと、また万一事業活動が中断した場合に目標復旧時間内に重要な機能を再開させ、業務中断に伴う顧客取引の競合他社への流出、マーケットシェアの低下、企業評価の低下などから企業を守るための経営戦略。バックアップシステムの整備、バックアップオフィスの確保、安否確認の迅速化、要員の確保、生産設備の代替などの対策を実施する」[(1)]ものである。ただし、BCPは単なる計画書を指すのではなく、事業継続マネジメント全般である「事業継続管理」（Business Continuity Management: BCM）の意味として用いる場合もある。

企業のICTへの依存度が高まっている今日では、BCP及びBCMの一環として、サイバーセキュリティインシデントや情報システム障害が発生した場合の対策を考えておくことが重要になっている。このため、情報セキュリティマネジメントにおいてもBCP及びBCM、特に情報システム運用継続計画（IT-BCP）の位置付けは非常に大きくなってきている[(2)]。

このような中、経済産業省では、2004年9月に商務情報政策局長の私的研究会として「企業における情報セキュリティガバナンスのあり方に関する研究会」が発足し、その成果として、「事業継続計画策定ガイドライン」等を策定し、2005年3月に公開している[(3)]。また、内閣府では、運営するウェブサイト「防災情報のページ」において「企業防災」の一環として「事業継続」に関する啓発コンテンツとともにガイドラインを掲載している[(4)]。さらに、中小企業庁も中小企業に向けたBCP策定運用指針を公開している[(5)]。

一方、BCPを策定したとしても、定期的な訓練等で対応方法の周知を徹底していないと、緊急時に普段実施していないことを正確に行うことは難しい。そのため、普段から関係者間で実際の体制や対応について確認しておく必要がある[(6)]。そこで、内閣サイバーセキュリティセンター（NISC）では、主に重要インフラ事業者を対象に、複数分野のサービスに影響する緊急事態を想定した演習「重要インフラにおける分野横断的演習（Critical Infrastructure Incident Response Exercise: CIIREX）」を2006年度から実施している。

これらの政府の取組とは別に、民間では、2006年に事業継続推進機構（Business Continuity Advancement Organization: BCAO）が設立されている。同機構は、国内外の個人及び企業、政府そのほかの団体に対して、「災害、事故、事件等のリスクの発生時における事業継続（BC）の取組みの推進に資する事業を行い、経済・社会的被害の軽減及び地域社会における災害・危機管理対策の充実を図り、もって国及び各地域の安全・安心・発展に寄与することを目的」[(7)]としている。また、同機構では、事業継続管理者や担当者の基礎知識習得の支援や、事業継続の実務経験者の専門性向上のための専門資格制度を構築・運用している[(8)]。

●事例研究

■中央省庁における情報システム運用継続計画ガイドライン

NISCでは、東日本大震災における政府機関の情報システムへの影響に関して調査・分析を行い、それを踏まえ2012年5月に「中央省庁における情報システムの運用継続計画ガイドライン」の改訂を実施した(9)。「第二次情報セキュリティ基本計画」（平成21年2月3日情報セキュリティ政策会議決定）の決定に従い、各政府機関は業務継続計画を策定するものとされており、本ガイドラインは府省庁の業務継続計画の情報システム版である「情報システム運用計画」を策定するためのものである。

●海外の状況、技術動向、制度、規制

■事業継続管理（BCM）の国際標準化

事業継続分野の国際協会である事業継続協会（The Business Continuity Institute: BCI）が2002年に「BCI Good Practice Guidelines（実践的なガイドライン）」を発行し、事業継続管理に関する包括的な概念・考え方を示した。これをもとに英国規格協会（British Standards Institution: BSI）が2003年にBCMガイドラインの一般仕様書「PAS56 Guide to Business Continuity Management」を発表し、欧州で広まったほか、日本でも日本規格協会（Japanese Standards Association: JSA）から邦訳「事業継続管理のための指針」が発行された。2006年11月にBSIがBS25999-1を正式に発行し、国際標準化機構（International Organization for Standardization: ISO）に国際標準として採用するように提案した。(10)

その後、BS25999-1をもとに事業継続マネジメントシステム（Business Continuity Management System: BCMS）の国際規格として、2012年5月にISO 22301:2012が発行され、2013年10月には、その日本版であるJIS Q 22301:2013が発行されている。

各国では、ISO 22301に基づくBCMSの第三者認証制度が運用されており、日本でも日本情報経済社会推進協会（JIPDEC）がISO 22301の要求事項への適合性について、認定機関（JIPDEC）から認定を受けた認証機関が評価を行う「BCMS適合性評価制度」を運用している(11)。

---

(1)　「事業継続」内閣府防災情報のページウェブサイト <http://www.bousai.go.jp/kyoiku/kigyou/keizoku/sk.html>
(2)　日本情報処理開発協会「事業継続管理（BCM）に関する調査報告書―BCM（BS25999）と関連領域の整理―」2007.3, pp.13-15. <http://www.isms.jipdec.or.jp/keirin/sw/18-H006.pdf>
(3)　「企業における情報セキュリティガバナンスのあり方に関する研究会報告書」2005.3. 経済産業省ウェブサイト <http://www.meti.go.jp/report/downloadfiles/g50331d00j.pdf>;「企業における情報セキュリティガバナンスのあり方に関する研究会 報告書 参考資料 事業継続計画策定ガイドライン」2005.3. 経済産業省ウェブサイト <http://www.meti.go.jp/report/downloadfiles/g50331d06j.pdf>
(4)　前掲注(1)
(5)　「中小企業BCP策定運用指針―緊急事態を生き抜くために―」中小企業庁ウェブサイト <http://www.chusho.meti.go.jp/bcp/>
(6)　「中小企業BCP策定運用指針―緊急事態を生き抜くために― 1.1BCP（事業継続計画）とは」中小企業庁ウェブサイト <http://www.chusho.meti.go.jp/bcp/contents/level_a/bcpgl_01_1.html>
(7)　「機構概要」事業継続推進機構ウェブサイト <http://www.bcao.org/gaiyou/>
(8)　事業継続推進機構「BCAO事業継続資格制度」2013.10. 事業継続推進機構ウェブサイト <http://www.bcao.org/shiken/pdf/shikakuseido.pdf>
(9)　内閣官房情報セキュリティセンター「中央省庁における情報システム運用継続計画ガイドライン―策定手引書（第2版）―」2012.5. <http://www.nisc.go.jp/active/general/pdf/itbcp1-1_2.pdf>
(10)　日本情報処理開発協会　前掲注(2), pp.2, 14.
(11)　日本情報経済社会推進協会「BCMS適合性評価制度の概要―経営者と管理者のための事業継続の手引き―」<http://www.isms.jipdec.or.jp/doc/bcmspanf.pdf>

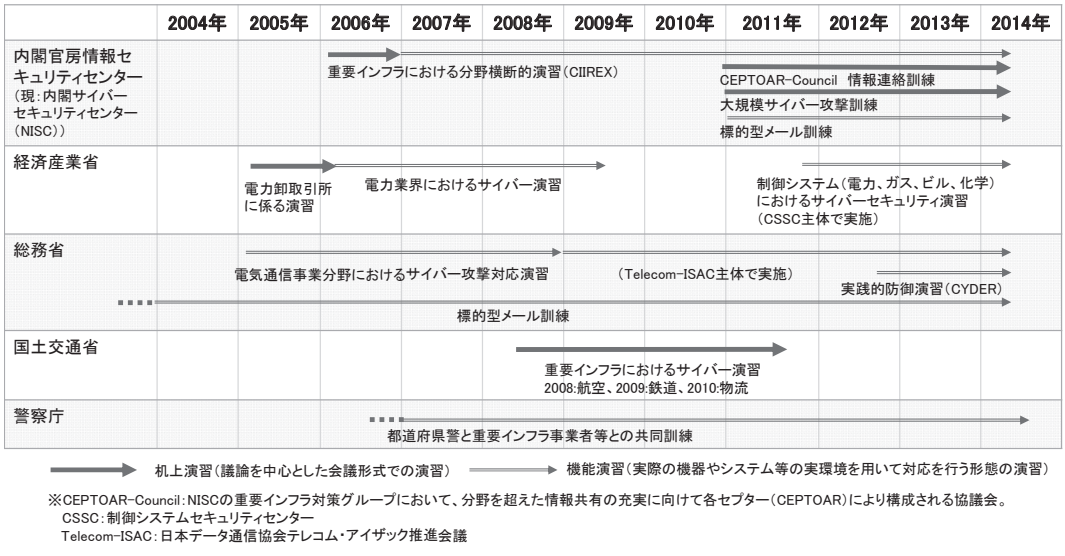
4.5　サイバー攻撃に備えた実践的演習

高度化するサイバー攻撃への備えとして、近年、官公庁が主催するサイバー演習が実施されている。主なサイバー演習として、重要インフラにおける分野横断的演習や、制御システムへのサイバー攻撃を想定したサイバーセキュリティ演習等がある。

サイバー演習とは、情報システムのインシデント発生を想定したシナリオを設定し、必要に応じて対応又は判断・対応について議論することで、情報システムにおけるインシデント対応体制・手順や、情報システムやサービスの稼働継続に関わる手順・規程（情報システム運用継続計画（IT-BCP）等）に関して、実行可能性や課題抽出を行うものである。

米国では、サイバー攻撃対処計画の改善や対処能力の向上を目的として、1990年代後半から多くのサイバー演習が実施されており、日本においても、図1に示すように様々な演習が近年実施されている。内閣官房情報セキュリティセンター（現：内閣サイバーセキュリティセンター（NISC））による重要インフラにおける分野横断的演習（CIIREX）は、2006年度から継続して実施されている。重要インフラ事業者における事業継続計画（BCP）等の実効性の確認や課題抽出を通じて、分野横断的な脅威に対する対応力の強化や官民の情報共有の方策検討を推進しており、9回目となる2014年度には重要インフラ13分野の事業者を中心に政府機関等、94組織348名が参加している(1)。また、経済産業省では、制御システムを対象としたサイバーセキュリティ演習を実施している。2012年度は経済産業省により電力・ガス・ビル分野を対象に、2013年度以降は制御システムセキュリティセンター（CSSC）により化学分野を対象に加えて実施されており(2)、模擬プラントを活用して、参加者が攻撃側・守備側に分かれて演習を行う手法が取り入れられている。ほかにも、官公庁及び重要インフラ事業者等のLAN管理者が参加して行われた総務省主催の実戦的サイバー防御演習（CYDER）や、総務省内での標的型メール訓練などが行われている(3)。

図1　国内の主なサイバー演習の実施状況



（出典）江連三香「増加する社会インフラを標的としたサイバー攻撃：5.　サイバー攻撃に備えた実践的演習」『情報処理』55巻7号, 2014.7, p.668.を基に三菱総合研究所作成。

●事例研究

■制御システムセキュリティセンター（CSSC）によるサイバーセキュリティ演習

CSSCでは、電力・ガス・ビル・化学分野において、2013年度から制御システムを対象としたサイバーセキュリティ演習を実施している。現場の担当者、技術者、関係するベンダ等が、制御システムにおけるセキュリティ上の脅威を認識し、セキュリティインシデント発生の検知手順や障害対応手順の妥当性について検証することを目的としており、各分野の業界団体や事業者、制御システムベンダ等が参加している。分野ごとの模擬プラントを用いて演習を実施しており、一部分野では模擬プラントを実際に攻撃するなどの手法により、脅威と対策効果の体感を通じた意識啓発を行っている。(4)

●海外の状況、技術動向、制度、規制

■米国国土安全保障省によるサイバー演習「Cyber Storm」

米国国土安全保障省（Department of Homeland Security: DHS）では、官（連邦・州政府・自治体）及び民間セクター（主に重要インフラ事業者）、各分野のISAC（Information Sharing and Analysis Center）(5)等が参加するサイバー演習「Cyber Storm」を実施している。2006年、2008年、2010年、2012～2013年の4回が実施されており、直近の「Cyber Storm IV」では、「サイバー対応力の評価」、「変化する脅威に対する対応プロセスの検証」、「連邦政府、州政府、国外組織、民間組織との情報共有の強化」に重点を置き、海外からも日本を含む10か国が参加した。(6)

■欧州ネットワーク情報セキュリティ庁（ENISA）によるサイバー演習「Cyber Europe」

欧州では、EUの機関であるENISAにより、EU及びEFTAの加盟国の関連省庁やCSIRT、情報機関、通信事業者等が参加して、大規模な複数の国にまたがるサイバー攻撃に対する欧州諸国の対応力の強化や連携方法の検証を目的とし、サイバー演習「Cyber Europe」が実施されている。2010年、2012年に実施されており、2014～2015年は3回に分けて実施されている。2014～2015年のサイバー演習には29の国と200組織から400人以上の専門家が参加する予定である。(7)

---

(1)　内閣官房情報セキュリティセンター「重要インフラにおける分野横断的演習の実施概要について―2014年度分野横断的演習―」2014.12.9. <http://www.nisc.go.jp/active/infra/pdf/bunya_enshu2014gaiyou.pdf>

(2)　制御システムセキュリティセンター「制御システムセキュリティの脅威と対策の動向およびCSSCの研究概要について（一般向け）」2015.2.2, pp.10, 23. <http://www.css-center.or.jp/pdf/about_CSSC.pdf>

(3)　総務省情報流通行政局情報セキュリティ対策室「総務省における人材育成に関する取組―実践的サイバー防御演習「CYDER」―」2014.6.18. <http://www.nisc.go.jp/conference/seisaku/jinzai/dai11/pdf/shiryou0203.pdf>; 総務省「平成23年度情報セキュリティ報告書」2012.5, p.12. <http://www.nisc.go.jp/active/general/pdf/10_soumu_h.pdf>

(4)　制御システムセキュリティセンター「サイバーセキュリティ演習」2014.6, pp.7, 14-15. <http://www.css-center.or.jp/pdf/cybersecurity-exercises_outline.pdf>

(5)　重要インフラ等の分野内でセキュリティに関する情報共有を行うための組織のこと。

(6)　“Cyber Storm: Securing Cyber Space.” Department of Homeland Security Website <http://www.dhs.gov/cyber-storm-securing-cyber-space>

(7)　European Union Agency for Network and Information Security, “Cyber Europe 2014-Questions and Answers,” October 2014. <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-europe/ce2014/cyber-europe-2014-information/briefing-pack/cyber-europe-2014-2013-questions-and-answers>

4.6　内部不正対策

情報セキュリティ対策においては、外部からのサイバー攻撃だけでなく、甚大な被害を生む可能性が高い内部不正も想定しなければならない。

日本ネットワークセキュリティ協会（JNSA）の「2012年情報セキュリティインシデントに関する調査報告書―個人情報漏えい編―」によれば、情報漏えいの原因は圧倒的に「管理ミス」（59.0%）や「誤操作」（20.1%）によるものが多く、「不正な情報持ち出し」や「内部犯罪・内部不正行為」はそれぞれ2.5%、1.3%と決して多くはない(1)。しかし、一般的に内部不正による情報漏えいは、公的機関に届けられることなく、内部で処理されてしまうこともあるため、公になっているのは、あくまで「氷山の一角」であり、実態は明らかになっていないと言える。特に、その企業独自の技術情報のような機密情報の場合は、届け出によって機密情報が公になることを避けるために、公的機関等に届けられないケースが多くあると考えられる(2)。

2014年にはベネッセコーポレーションから3500万件を超える個人情報が流出するという、国内で公になっている事例としては過去最大規模の個人情報流出事件が発生し、しかも、システムの保守・管理委託先に派遣されていたシステムエンジニアという内部者が容疑者として逮捕される事件が発生している。この事件のように、内部の、特にシステムを熟知している者による犯行の場合は、被害規模が甚大になる危険性が極めて高い。(3)

このような状況の一方で、2010年3月に、社会安全研究財団（現：日工組社会安全財団）は「情報セキュリティにおける人的脅威対策に関する調査研究報告書」を公開している。これは、内部犯行者の特性や動機に関する米国の調査研究状況について整理するとともに、警察のデータを利用した詳細な事例調査を行い、内部犯行について類型化などを行うことで、事案発生過程やその原因を把握し、対策を検討したものである(4)。

また、情報処理推進機構（IPA）は、情報漏えい元の組織に所属する幅広い人々を対象に意識調査を行い、内部不正の誘発要因やそれに対する抑止・防止対策を考察した調査結果を「組織内部者の不正行為によるインシデント調査―調査報告書―」として2012年7月に公開している。社員向けアンケート結果では、社内システムの操作記録が残ることが内部犯行の抑止に重要であり、そのために、内部不正者を特定するためのアカウントの管理及びアクセス権限の設定を適切に行うことが必要であると指摘している(5)。さらにIPAではこの調査結果を踏まえ、内部不正に関する知見を有する様々な分野の有識者からなる「組織における内部不正防止ガイドライン検討委員会」を設置し、その成果として、「組織における内部不正防止ガイドライン」(6)を2013年3月25日に公開している。同ガイドラインでは、組織における内部不正を防ぐための管理の在り方について、基本方針から、資産管理、物理的管理、技術的管理、証拠確保、人的管理、コンプライアンス、職場環境、事後対策、組織の管理など10の観点のもと、合計30項目からなる具体的な対策を示している。例えば、証拠確保の観点からは、「情報システムにおけるログ・証跡の記録と保存」、「システム管理者のログ・証跡の確認」等の対策が示されている。なお、2014年9月26日に同ガイドラインの改訂版が公開されている。

●事例研究

■内部犯行による情報流出

内部犯行によって、国内企業の機密情報が流出する事件が起きている。2006年8月、光学機器メーカーであるニコンのグループ企業の元研究員が軍事用技術を在日ロシア通商代表部のロシア人に渡したとして逮捕される事件が発生した（起訴猶予処分(7)）。また、2014年3月、東芝と業務提携していた米国の半導体メーカーの日本人技術者が東芝の研究情報を不正に持ち出して韓国の半導体大手のSKハイニックスに提供したとして逮捕される事件が起きている（起訴、一審公判中(8)。損害賠償裁判については、企業間は2014年12月に和解成立。）。これらの事件を踏まえ、2014年5月には「営業秘密保護法」制定の必要性に関する質問主意書が国会に提出されている(9)。

●海外の状況、技術動向、制度、規制

■米国CERT/CCのInsider Threat Study

米国のインシデント対応機関であるCERT/CCでは、150件の内部犯行事例を収集・分析し、その結果を2009年に「Common Sense Guide to Prevention and Detection of Insider Threat」として公表した。同報告書では、内部犯行の予兆の検知、犯行に対する防護のためのベストプラクティスを紹介している。2012年には、更新版として「Common Sense Guide to Mitigating Insider Threats 4th Edition」が公表されている(10)。

また、2008年の報告「Insider Threat Study」によれば、悪意のある行動をする内部犯行者の多くが似た特徴を持つ人物であることや、処罰など従業員にとって好ましくない出来事が破壊行為の発生確率を上げる、内部犯行者の犯行の兆候を示す振舞いや技術的な前兆が見落とされているなどのポイントが紹介されている。(11)

(1)　日本ネットワークセキュリティ協会セキュリティ被害調査ワーキンググループほか「2012年情報セキュリティインシデントに関する調査報告書―個人情報漏えい編―第1.1版」2014.7.7, p.16. <http://www.jnsa.org/result/incident/data/2012incident_survey_ver1.1.pdf>

(2)　社会安全研究財団情報セキュリティにおける人的脅威対策に関する調査研究会「情報セキュリティにおける人的脅威対策に関する調査研究報告書」2010.3, p.2. <http://www.syaanken.or.jp/wp-content/uploads/2012/05/cyber2203_01.pdf>

(3)　「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>

(4)　社会安全研究財団情報セキュリティにおける人的脅威対策に関する調査研究会　前掲注(2), pp.66-67.

(5)　情報処理推進機構「組織内部者の不正行為によるインシデント調査―調査報告書―」2012.7.17, p.66. <http://www.ipa.go.jp/files/000014169.pdf>

(6)　情報処理推進機構「組織における内部不正防止ガイドライン」2014.9.26. <http://www.ipa.go.jp/files/000041054.pdf>

(7)　「ロシア側に機密部品、ニコン元研究員、起訴猶予」『日本経済新聞』2007.2.23.

(8)　「元技術者に懲役6年求刑、東芝データ漏洩、検察「身勝手で悪質」」『日本経済新聞』2015.2.14.

(9)　「営業秘密保護法制定の必要性に関する質問主意書」（第186回国会参議院質問第108号）2014.5.26. 参議院ウェブサイト <http://www.sangiin.go.jp/japanese/joho1/kousei/syuisyo/186/syup/s186108.pdf>

(10)　George Silowash et al.,“Common Sense Guide to Mitigating Insider Threats 4th Edition,”December 2012. Software Engineering Institute, Carnegie Mellon University Website <http://resources.sei.cmu.edu/asset_files/TechnicalReport/2012_005_001_34033.pdf>

(11)　Eileen Kowalski et al.,“Insider Threat Study: Illicit Cyber Activity in the Information Technology and Telecommunications Sector,”January 2008. Software Engineering Institute, Carnegie Mellon University Website <http://resources.sei.cmu.edu/asset_files/WhitePaper/2008_019_001_52266.pdf>

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。