Ⅱ-2
情報系におけるサイバーセキュリティ

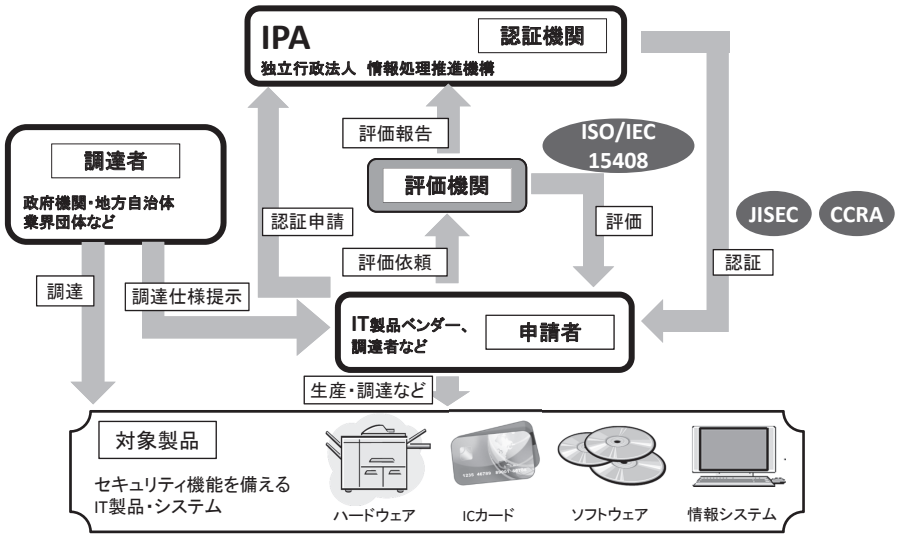
2.1　情報セキュリティに関する国際基準・認証

情報セキュリティの観点から、情報技術に関連した製品及びシステムが適切に設計され、その設計が正しく実装されているかを第三者が評価及び認証する仕組みが整備されており、国際標準に基づいてITセキュリティ評価及び認証制度（JISEC）などが運用されている。

情報セキュリティの観点から、情報技術に関連した製品及びシステムが適切に設計・実装されているかを第三者が評価及び認証する仕組みは、政府機関を含む利用者・調達者が適切な情報セキュリティ対策を確保することを目的として、整備が行われてきた。また、近年では、サプライチェーンのセキュリティの観点から、調達品をブラックボックスとして扱うのではなく、セキュリティが確保された製品として調達することが求められており、このためにも第三者による認証制度が重要となっている。

現在、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に基づいて第三者が評価・認証する「ITセキュリティ評価及び認証制度（Japan Information Security Evaluation and Certification Scheme: JISEC）」が情報処理推進機構（IPA）により図1に示す体制で運用されている。評価で用いられるセキュリティ評価基準ISO/IEC 15408は、コモンクライテリア（Common Criteria: CC）として開発され、後に国際標準となったものである。製品の開発者は、第三者である評価機関から、実装したセキュリティ機能の保証がCCに準拠したレベルかどうかの評価を受け、その評価結果が国際標準に適合していることを認証機関が調査し、適合している場合にはその製品に認証が与えられる。なお、CCに基づき評価・認証された製品は、「ITセキュリティ分野における国際相互承認に関するアレンジメント（Common Criteria Recognition Arrangement: CCRA）」に加盟する各国の認証機関により公表され、その評価認証の結果を関係国間で相互承認することとなっている。(1)

図1　ITセキュリティ評価及び認証制度の運用体制



（出典）「評価認証制度（JISEC）概要」情報処理推進機構ウェブサイト <https://www.ipa.go.jp/security/jisec/scheme/index.html> を基に三菱総合研究所作成。

なお、海外の同種の制度と相互承認されている制度ではないものの、国内では第三者による

認証制度として、ISO/IEC 19790:2006（JIS X 19790:2007）に基づく「暗号モジュール試験及び認証制度（Japan Cryptographic Module Validation Program: JCMVP）」も運用されている。JCMVPは、「暗号モジュールが、その内部に格納するセキュリティ機能並びに暗号鍵及びパスワード等の重要情報を適切に保護していることを、第三者が試験・認証する」制度であり、IPAにより運用されている(2)。

●事例研究

■コモンクライテリア（CC）の活用状況

CCは多くの国で政府調達基準として利用されており、日本においても、政府の「サイバーセキュリティ戦略」の年次計画である「サイバーセキュリティ2013」において、安全性・信頼性の高いIT製品等の利用推進及び政府調達における情報セキュリティの確保が求められている(3)。経済産業省が公開している「IT製品の調達におけるセキュリティ要件リスト」では、指定したセキュリティ要件が満たされていることの確認手段として、CCのような国際基準に基づく第三者認証の活用を推奨している。同リストでは、対象となる製品分野として、デジタル複合機（MFP）やファイアウォール、侵入検知／防止システム（IDS/IPS）、OS（サーバOSに限る）、データベース管理システム（DBMS）、スマートカード（ICカード）の6分野を指定している(4)。

認証を取得したIT製品・システムは公開されており(5)、2014年9月時点で認証件数は累計429件、CCRA加盟国26か国中4位となっている(6)。なお、JISECは2001年4月から製品評価技術基盤機構（NITE）を認証機関として運用が開始されたが、2004年4月に、IPAに認証業務及び運営が移管された(7)。

●海外の状況、技術動向、制度、規制

■ドイツ政府での調達におけるCCの活用

ドイツでは、連邦政府の情報セキュリティ担当組織であるBSI（Bundesamt für Sicherheit in der Informationstechnik）がセキュリティ評価認証制度に関わる責任と権限を与えられ、制度を運用している(8)。連邦政府が調達するeIDカードやePassportで使われる電子IDに対して、ISO/IEC 15408に基づいたセキュリティ要求仕様である「プロテクションプロファイル（Protection Profile: PP）」をBSIが策定し、このPPに従った調達を実施している(9)。

---

(1)　「評価認証制度（JISEC）概要」情報処理推進機構ウェブサイト <https://www.ipa.go.jp/security/jisec/scheme/index.html>
(2)　「情報セキュリティ認証関連」情報処理推進機構ウェブサイト <http://www.ipa.go.jp/security/certification/>
(3)　情報セキュリティ政策会議「サイバーセキュリティ2013」2013.6.27, pp.8-9. <http://www.nisc.go.jp/active/kihon/pdf/cs2013.pdf>
(4)　経済産業省「IT製品の調達におけるセキュリティ要件リストを策定しました」2014.5.19, pp.1, 3. <http://www.meti.go.jp/press/2014/05/20140519003/20140519003.pdf>
(5)　「認証製品リスト」2015.2.23. 情報処理推進機構ウェブサイト <http://www.ipa.go.jp/security/jisec/certified_products/cert_list.html>
(6)　「ITセキュリティ分野における国際相互承認アレンジメントが改正されました」2014.9.10. 経済産業省ウェブサイト <http://www.meti.go.jp/press/2014/09/20140910001/20140910001.html>
(7)　前掲注(1)
(8)　Federal Office for Information Security,“BSI 7138: Technical information on the IT security certification of products, protection profiles and sites (including confirmations in accordance with SigG),”Version 2.1, November 5, 2012, p.3. <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/7138_e_pdf.pdf?__blob=publicationFile>
(9)　“Technical guidelines and protection profiles regarding electronic ID documents.”Federal Office for Information Security Website <https://www.bsi.bund.de/EN/Topics/ElectrIDDocuments/TRprotect/protect_node.html>

2.2　スマートフォンのセキュリティ

スマートフォンやタブレット端末などの携帯端末（スマートデバイス）の利用が広まる中、特有のセキュリティ問題が深刻化している。この状況を踏まえ、内閣サイバーセキュリティセンター（NISC）や総務省などが取組を行っているほか、民間では日本スマートフォンセキュリティ協会がガイドラインの策定などを進めている。

スマートフォンやタブレット端末などの携帯端末（スマートデバイス）の利用が広まっている。内閣府が行っている消費動向調査によると、2014年3月末のスマートフォンの世帯普及率（一般世帯）は54.7%、タブレット端末が20.9%となっている(1)。また、企業において個人が所有するスマートデバイスを業務で利用するBYOD（Bring Your Own Device）を含め、スマートデバイスの業務利用が広がっている(2)。

その一方で、スマートフォンのセキュリティ問題も顕在化している。特にスマートフォン向けのアプリケーション（以下「アプリ」という。）の中には利用者が想定していない動作をするものがあり、架空の利用料金の請求画面を繰り返し表示させる不正なアプリによる架空料金請求や、便利な機能を持つアプリに偽った不正なアプリによる個人情報の不正収集などの事例が発生している(3)。こういった不正なアプリは急増しており、GoogleのAndroidをOS（基本ソフト）として搭載しているスマートフォン向けの不正アプリの累積検出数は2014年3月には200万種を突破し、うち約65万種が2014年1月から3月の増加分となっている(4)。そのため、被害の多くはAndroidをOSとして搭載しているスマートフォンで発生しているが、AppleのiOSを対象としたマルウェアの事例もあり、それぞれの特徴に応じた対策を講じることが求められている(5)。

このような中、内閣サイバーセキュリティセンター（NISC）は、運営する「国民を守る情報セキュリティサイト」において「スマートフォン利用者の方へ」と題した注意喚起及び啓発のページを用意している(6)。また、総務省では2011年から「スマートフォン・クラウドセキュリティ研究会」を開催し、その成果を2012年6月に「スマートフォンを安心して利用するために実施されるべき方策」として公開している(7)。この中で、利用者が最低限とるべき情報セキュリティ対策として、紛失や盗難への対策、他人による不正利用防止対策といった従来の携帯電話と同様の対策に加え、一般的なパソコンと同様に「OS（基本ソフト）を更新」、「ウイルス対策ソフトの利用を確認」、「アプリケーションの入手に注意」という「スマートフォン情報セキュリティ3か条」が提示されている(8)。このほかにも、情報処理推進機構（IPA）により、啓発コンテンツとして「スマートフォンのセキュリティ＜危険回避＞対策のしおり」(9)や漫画などを利用した「I♥スマホ生活」(10)などが公開されており、利用者への普及啓発が進められている。

これらの政府の活動とは別に、民間では日本スマートフォンセキュリティ協会（JSSEC）が、スマートフォンなどの業務利用に関するセキュリティガイドラインやアプリのセキュア設計・セキュアコーディングガイドなどの文書を公開している(11)。また、ウイルス検知ソフトのベンダからは、スマートフォン向けのセキュリティ対策ソフトも提供・販売されるようになってきている。

●事例研究

■日本スマートフォンセキュリティ協会（JSSEC）

2011年5月に発足したJSSECは、スマートフォンの安全な利活用を図るとともに、サービス提供者が安心して事業推進を行える環境を整備することを目的に、通信事業者や機器メーカー、アプリケーション開発事業者、サービス提供ベンダなどの提供者に加え、利用企業及び関連団体によって設立された民間の非営利団体である(12)。JSSECでは「スマートフォン企業利用実態調査」を行っているほか、「スマートフォン＆タブレットの業務利用に関するセキュリティガイドライン」の公開など、スマートフォンの安全利用促進のための利用方法の検討を行っている。また、「スマートフォンネットワークセキュリティ実装ガイド」や「Androidアプリのセキュア設計・セキュアコーディングガイド」の公開など、スマートフォンのセキュリティに関する技術的な調査・研究・議論を進めるほか、セキュリティリテラシー向上のための活動を行っている(13)。

●海外の状況、技術動向、制度、規制

■米国「キルスイッチ」機能の義務化への動き

2014年8月25日付米ウォール・ストリート・ジャーナル紙の報道“California Smartphone ‘Kill Switch’ Bill to Become Law”によると、スマートフォンの盗難が多発する米国において、盗難後に遠隔から端末を無効化できる「キルスイッチ（Kill Switch）」機能によって盗難率が低下しているとの法執行機関の発表を受け、カリフォルニア州では、2015年7月1日以降、製造・販売されるあらゆるスマートフォンにキルスイッチ機能を標準搭載することが義務付けられることになった。キルスイッチ機能の搭載義務化は、米国ではミネソタ州に次いでカリフォルニア州が2番目である(14)。なお、日本ではキルスイッチ機能の搭載は義務付けられていない。

---

(1)　「平成26年3月実施調査結果：消費動向調査」2014.4.17. 内閣府ウェブサイト<http://www.esri.cao.go.jp/jp/stat/shouhi/2014/201403shouhi.html#durables>
(2)　日本情報経済社会推進協会「特集「企業IT利活用動向調査2014」にみるIT化現状」『JIPDEC IT-Report』2014 Spring, 2014.5, pp.17-18. <http://www.jipdec.or.jp/WSR/itreport_spring.pdf>
(3)　「スマートフォン利用者の方へ 特徴やリスクって？」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/smartphone/risk.html>
(4)　トレンドマイクロ「TrendLabs2014年第1四半期セキュリティラウンドアップ新たな獲物を見つけたサイバー犯罪者―狙われたPOSシステムと仮想通貨―」2014.5.20, pp.31-32. <http://www.trendmicro.co.jp/cloud-content/jp/pdfs/security-intelligence/threat-report/pdf-2014q1-20140520.pdf?cm_sp=Corp-_-sr-_-2014Q1>
(5)　スマートフォン・クラウドセキュリティ研究会「スマートフォン・クラウドセキュリティ研究会最終報告―スマートフォンを安心して利用するために実施されるべき方策―」2012.6.29, pp.11-12, 21. 総務省ウェブサイト<http://www.soumu.go.jp/main_content/000166095.pdf>
(6)　「スマートフォン利用者の方へ あなたのスマートフォンの情報セキュリティは大丈夫ですか？」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/smartphone/>
(7)　スマートフォン・クラウドセキュリティ研究会　前掲注(5)
(8)　同上, p.53.
(9)　情報処理推進機構「スマートフォンのセキュリティ＜危険回避＞対策のしおり」2012.6.8. <http://www.ipa.go.jp/files/000011456.pdf>
(10)「I♥スマホ生活 スマートフォンをもっと安全にもっと快適に！」情報処理推進機構ウェブサイト <http://www.ipa.go.jp/security/keihatsu/love_smartphone_life/>
(11)「部会・WGからの報告成果物」日本スマートフォンセキュリティ協会ウェブサイト <http://www.jssec.org/report>
(12)「JSSECについて」日本スマートフォンセキュリティ協会ウェブサイト <http://www.jssec.org/about>
(13)「活動内容」日本スマートフォンセキュリティ協会ウェブサイト <https://www.jssec.org/activities>
(14)　Nick Shchetko, “California Smartphone ‘Kill Switch’ Bill to Become Law,” *Wall Street Journal*, August 25,2014. <http://blogs.wsj.com/digits/2014/08/25/california-smartphone-kill-switch-bill-to-become-law/>

2.3　クラウドのセキュリティ

クラウドが普及する中、クラウド特有のセキュリティ対策が求められている。この状況を踏まえ、経済産業省は「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」を、総務省は「クラウドサービス提供における情報セキュリティ対策ガイドライン」を公表するなどの取組を行っている。

データやソフトウェアをネットワーク経由でサービスとして提供するクラウドサービスの利用が広まっている。総務省が行った2013年の調査によれば、一部でもクラウドサービスを利用していると回答した企業の割合は33.1%で、2012年の28.2%から4.9ポイントの上昇を見せている(1)。しかし、クラウドサービスの性質上、サーバ内でのデータの消失や意図しない者とのデータ共有といったリスクがあり、2012年には実際にファーストサーバ株式会社が提供するクラウドサービスで顧客のデータを大量に消失する事故が起きた(2)。

このようなクラウドサービスの利用の拡大やリスクの高まりに対し、早くからセキュリティに関する取組が行われてきた。経済産業省は、クラウドサービスの情報セキュリティ上の不安を減少させ、利用を促進するため、利用者がクラウドサービスを利用する際に考慮すべき事項などをまとめた「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」を2011年4月に公表した(3)。その後2014年3月に、クラウドサービスを取り巻く環境の変化を踏まえ、内容を追加する形でガイドラインを改訂し(4)、併せて活用方法やクラウド契約時の契約書やサービスレベル合意書（SLA）等について解説した「クラウドセキュリティガイドライン活用ガイドブック」を公開した(5)。

また、日本セキュリティ監査協会（JASA）は、グローバルなクラウドセキュリティ監査の利用促進を目的とした経済産業省の委託事業の成果として「クラウド情報セキュリティ管理基準」などを2012年に公表している(6)。2013年4月には、「JASA－クラウドセキュリティ推進協議会」（JCISPA）が発足し(7)、「クラウド情報セキュリティ管理基準」、「クラウド情報セキュリティ監査技術ガイド」等の策定及び改訂を行っており、クラウド事業者向けの「クラウド情報セキュリティ監査制度」が始まっている(8)。

一方、総務省は、「クラウドサービス提供における情報セキュリティ対策調査検討会」における結果を踏まえ、2014年4月に、クラウドサービス提供事業者が留意すべき情報セキュリティ対策に関する「クラウドサービス提供における情報セキュリティ対策ガイドライン」を公表している。このガイドラインでは、サービス提供事業者と利用者との間で、責任の分担設定などあらかじめ取り決めておくべき事項が提示されているほか、クラウド提供事業者間でサービス提供に必要な技術仕様、運用手順などについて事前に調整することや、情報資産の分類やアクセス制御、情報の転送などに関する方針について適切に設定することを推奨している。(9)

●事例研究

■国内のクラウドサービスに関連した事故

クラウドサービス上のデータの情報漏えいやデータの消失など、国内においてもクラウドサービスに関連した事故が起こっている。2012年6月にはファーストサーバ株式会社のクラウドサービスにおいて、顧客の大量のデータの消失とともに、情報漏えいが発生し、データの消失件数は5,676件、情報漏えい被害が想定される契約者の最大範囲は2,359者に上った(10)。2013年には、メール共有サービス「Googleグループ」による情報漏えいも相次いで発生した。同サービスを利用していた複数の省庁や教育機関において、不適切なメールの公開設定により、関係者間のメールが同サービスの利用者全員に公開状態となり、機密情報が漏えいした(11)。

●海外の状況、技術動向、制度、規制

■米国クラウドセキュリティアライアンス

米国クラウドセキュリティアライアンス（Cloud Security Alliance: CSA）は、クラウドコンピューティングのセキュリティのためのベストプラクティスの普及を目的に、2008年に設立された非営利団体である(12)。2009年に発表した「クラウドセキュリティガイダンス（Security Guidance for Critical Areas of Cloud Computing）」はクラウドのセキュリティ課題に関する体系的なレポートとして世界的に注目を集め、2011年にはその改訂版も発表している(13)。

CSAは、2010年に日本支部として日本クラウドセキュリティアライアンス（CSAジャパン）(14)を設置（当時は任意団体、現在は一般社団法人）したほか、経済産業省所管の情報処理推進機構（IPA）と相互協力協定を締結している(15)。

(1)　総務省編「第2部第5章第4節クラウドサービスの利用動向」『平成26年版情報通信白書―ICT白書―』日経印刷, 2014, p.354. <http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h26/pdf/26honpen.pdf>
(2)　ファーストサーバ株式会社第三者調査委員会「調査報告書（最終報告書）（要約版）」2012.7.31, p.3. <http://support.fsv.jp/urgent/pdf/fs-report.pdf>
(3)　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」2011.4.1. <http://www.meti.go.jp/press/2011/04/20110401001/20110401001-3.pdf>
(4)　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」2014.3.14, p.1. <http://www.meti.go.jp/press/2013/03/20140314004/20140314004-2.pdf>
(5)　経済産業省「クラウドセキュリティガイドライン活用ガイドブック 2013年度版」2014.3.14. <http://www.meti.go.jp/press/2013/03/20140314004/20140314004-3.pdf>
(6)　「2011年度経済産業省受託事業 クラウドセキュリティ監査」2012. 日本セキュリティ監査協会ウェブサイト <http://www.jasa.jp/information/result.html?key=2011>
(7)　日本セキュリティ監査協会「「JASA－クラウドセキュリティ推進協議会」の発足について」2013.4.25. <http://www.jasa.jp/news/downf/news_20130425.pdf>
(8)　「主な活動内容」JASA－クラウドセキュリティ推進協議会ウェブサイト <http://jcispa.jasa.jp/about/activity/>
(9)　総務省「クラウドサービス提供における情報セキュリティ対策ガイドライン―利用者との接点と事業者間連携における実務のポイント―」2014.4. <http://www.soumu.go.jp/main_content/000283647.pdf>
(10)　ファーストサーバ株式会社第三者調査委員会　前掲注(2), pp.3, 6, 13.
(11)　情報処理推進機構「インターネットサービス利用時の情報公開範囲の設定に注意！」2013.10.1, p.1. <https://www.ipa.go.jp/files/000034678.pdf>
(12)　“About.”Cloud Security Alliance Website <https://cloudsecurityalliance.org/about/>
(13)　Cloud Security Alliance,“Security Guidance for Critical Areas of Focus in Cloud Computing V3.0,”November 14, 2011. <https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf>
(14)　「CSAジャパンについて」日本クラウドセキュリティアライアンスウェブサイト <http://www.cloudsecurityalliance.jp/organization.html>
(15)　情報処理推進機構「クラウドセキュリティアライアンスと独立行政法人情報処理推進機構の相互協力協定の締結について」2010.6.7. <https://www.ipa.go.jp/files/000008713.pdf>

2.4　ビッグデータ

通信やデバイスの向上に伴い、多種多量なデータが収集、蓄積されるようになり、ビッグデータとしてビジネスに利活用する事例が増えている。一方、個人情報を含むパーソナルデータの扱いに関するセキュリティやプライバシーの問題が発生しており、運用ルールや技術が検討されている。

ビッグデータとは多種多量なデータを意味しており、通信やデバイスなどの技術的な発展に伴い、ビッグデータは収集、蓄積され、リアルタイムに分析されるようになっている。収集、蓄積された大量のデータを分析することにより、ビジネス面で効率化や顧客満足度向上などにつながる効果が期待されている。具体的なビッグデータの利用方法としては、過去のデータの傾向に基づく将来予測や異常の検知、あるいは、過去の行動から推定される利用者個人のニーズに合わせたサービスの提供などが想定されている。ただし、ビッグデータとは名称のとおり大量のデータを意味しており、従来から分析されている、論理的な構造や意味を持つ構造化データ（コンビニエンスストアやスーパー等のレジで収集されるPOS（Point of Sales）データや各企業内で管理されている顧客や財務に関するデータ等）を含んでいる。一方でビッグデータは多様なデータとして、これまであまり分析、活用されていない非構造化データも対象としている。具体例としては、音声、画像、映像などのデータ、ブログやSNS等のソーシャルメディアに書き込まれるデータ、GPSを用いた位置データや加速度データ等の端末で使われている各種センサのデータが挙げられる。構造化データよりも非構造化データの方が圧倒的に多く、非構造化データに注目が集まっている。(1)

我が国におけるビッグデータを活用する経済効果は、総務省の推計（いずれも年間）によれば、流通業では販売促進効率化効果が約9894億円、発注量最適化効果が約1635億円とされている。製造業では、リモート監視によるメンテナンス人件費の効率化効果が4兆7380億円、インフラの維持管理、運用という観点では、橋梁の予防保全による延命効果が約2700億円、渋滞解消に伴う燃費向上効果が約1兆1600億円と推計されている。(2)

ビッグデータには個人に関する情報やそれに相当するデータが含まれているケースも多い。個人に関する大量の情報が集積、利用されることによる個人情報及びプライバシーの保護に関する不安も顕在化しており、「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）では保護できないケース、あるいは、利用時に問題が発生し、事業者が社会的な批判を受けるケースも見られる。例えば、東日本旅客鉄道がSuica乗降履歴データを変換したものを日立製作所に提供しようとして批判を浴び、取り止めたケースもある(3)。

日本政府は、パーソナルデータの円滑な利活用と個人情報及びプライバシーの保護を両立する事業環境を整備するために、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）の下に「パーソナルデータに関する検討会」を設置した。同検討会の技術検討ワーキンググループは、匿名化技術を適用しても個人が特定されるリスクが残り、リスクを踏まえて利活用を行うためには、制度の整備が必要とした(4)。同検討会の取りまとめを踏まえ、IT総合戦略本部は2014年6月に「パーソナルデータの利活用に関する制度改正大綱」(5)を決定し、そこでは、本人の同意がなくてもデータを利活用できる枠組みの導入や自主ルールの実効性のある運用がなされているかについて立入検査等をする権限を持つ第三者機関の整備などの方針が示された。

●事例研究

■モバイル空間統計

NTTドコモが提供する「モバイル空間統計」は、携帯電話が接続する基地局が持つ位置登録情報を利用し、各基地局がカバーする範囲に存在する端末の契約者に関する属性（年齢、性別、住所）に基づいて端末の位置を集計し、地理的な人口分布を1時間ごとに推計した情報である。公共分野の防災計画や都市設計、産業分野の商圏や通行量の調査に利用できる。NTTドコモは、契約者のプライバシーを保護するため、運用データ（位置登録情報及び属性情報）に対して、「運用データから氏名や電話番号、生年月日などの識別情報を取り除く」非識別化処理、統計的な「集団に関する情報」を導出する集計処理、「集計結果に小人数エリアの数値が含まれないようにする」秘匿処理をするほか、利用停止手続等を定めたガイドラインを公表している(6)。

●海外の状況、技術動向、制度、規制

■米国政府におけるビッグデータとプライバシーに関する報告書

2014年1月、オバマ大統領がビッグデータとプライバシーに関する包括的な見直しを指示し、同年5月にジョン・ポデスタ（John Podesta）大統領顧問を中心とする検討メンバーが、「ビッグデータ：機会を逃さず、価値を守る」(7)と題した報告書を提出した。同報告書では、Apple、Facebook、Googleなど関係企業との意見交換の結果等を踏まえ、ビッグデータの社会的、経済的な様々な可能性を示しつつ、プライバシーや社会的差別等が発生する懸念があることを指摘している。ビッグデータの便益を享受できるよう、例えば、①「消費者プライバシー権利章典」の促進、②「全国データ違反法」（National Data Breach Legislation）の成立、③プライバシー保護を非米国市民に拡大、④学校で生徒に関して収集されたデータが教育目的で使用されることを保証、⑤差別をなくすために技術的な専門知識を拡大、⑥「電気通信におけるプライバシー保護法」（Electronic Communications Privacy Act: ECPA）」の改正の6項目を提言している。

また、大統領科学技術諮問会議（President's Council of Advisors on Science and Technology: PCAST）では、技術的な観点から前述の報告書を補完する報告書「ビッグデータとプライバシー：技術的展望」(8)を公表している。

---

(1)　総務省編「第1部第1章第3節ビッグデータの活用が促す成長の可能性」『平成25年版情報通信白書―ICT白書―』日経印刷, 2013, pp.143-144. <http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h25/pdf/25honpen.pdf>

(2)　同上, pp.171-173.

(3)　東日本旅客鉄道「Suicaに関するデータの社外への提供について」2013.7.25, p.1. <http://www.jreast.co.jp/press/2013/20130716.pdf>

(4)　技術検討ワーキンググループ「技術検討ワーキンググループ報告書」2013.12.10, p.22. <http://www.kantei.go.jp/jp/singi/it2/pd/dai5/siryou2-1.pdf>

(5)　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.7-9. <http://www.kantei.go.jp/jp/singi/it2/info/h260625_siryou2.pdf>

(6)　「モバイル空間統計に関する情報」NTTドコモウェブサイト <https://www.nttdocomo.co.jp/corporate/disclosure/mobile_spatial_statistics/>;「モバイル空間統計ガイドライン」NTTドコモウェブサイト <https://www.nttdocomo.co.jp/corporate/disclosure/mobile_spatial_statistics/guideline/>

(7)　大統領行政府（次世代パーソナルサービス推進コンソーシアムほか訳）『ビッグデータ：機会を逃さず、価値を守る』2014. 次世代パーソナルサービス推進コンソーシアムウェブサイト <https://www.coneps.jp/contents/product_002.pdf>（原書名:Executive Office of the President, *Big Data: Seizing Opportunities, Preserving Values*, May 2014. <http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf>）

(8)　Executive Office of the President, President's Council of Advisors on Science and Technology, "Report to the President: Big Data and Privacy: A Technological Perspective," May 2014. <http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.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。