パーソナルデータの利活用に関する制度改正の基本的な考え方について

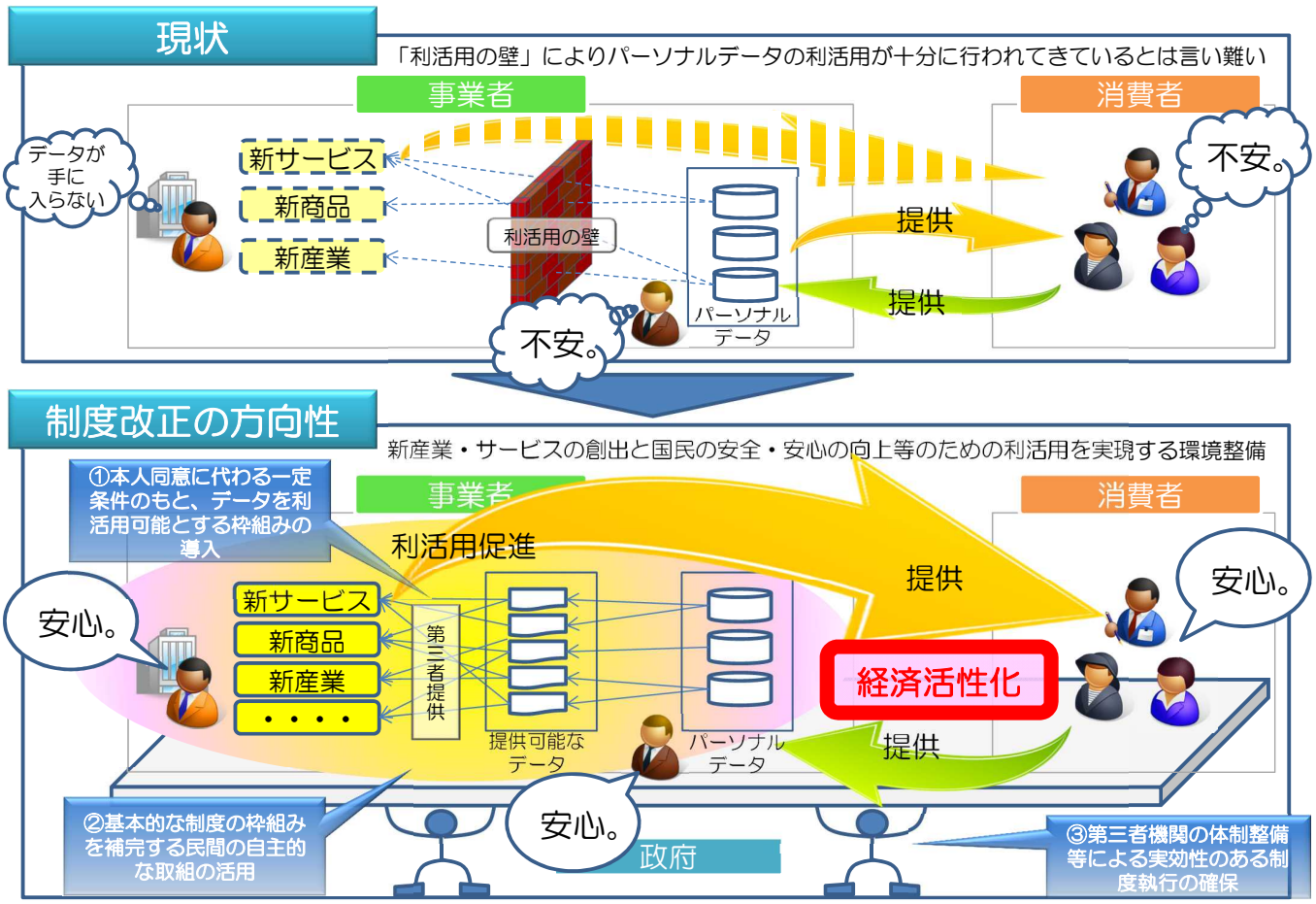
2014.6

パーソナルデータの利活用に関する制度改正について 1

基本的考え方

- 情報通信技術の進展により、多種多様・膨大なパーソナルデータが収集・分析されてきているが、その利活用に取り組む事業者が、特に個人の権利利益侵害に係る問題は発生させていないものの、個人情報として取り扱うべき範囲の曖昧さ（グレーゾーン）のために社会的な批判を懸念して、利活用に躊躇するという「利活用の壁」が出現しており、これまで、パーソナルデータの利活用が十分に行われてきているとは言い難い。
- このような現状に鑑み、政府の成長戦略においては、データ利活用による経済再生を一つの柱として掲げており、特に利用価値が高いとされるパーソナルデータについて、事業者の「利活用の壁」を取り払い、これまでと同様に個人の権利利益侵害を未然に防止しつつ、新産業・サービスの創出と国民の安全・安心の向上等のための利活用を実現する環境整備を行うことが求められている。
- これが今回の制度改正の主な目的・理由であり、制度改正により実現する新たな枠組み・ルールのポイントは、以下の３点である。
  - ① パーソナルデータの利活用は、目的外利用や第三者提供において大きな効果をもたらすことから、それらを本人の同意に代わる一定条件のもとで行うことを可能とする枠組みを導入する。
  - ② グレーゾーンの内容や、個人の権利利益の侵害の可能性・度合いは、情報通信技術の進展状況や個人の主観など複数の要素により時代とともに変動するものであることから、これに機動的に対応可能とするため、法律では大枠のみ定め、具体的な内容は政省令、規則及びガイドライン並びに民間の自主規制により対応するものとする。
  - ③ バランスのよい保護及び利活用の推進に向けて、法令や民間の自主規制を実効性あるものとして執行するために、独立した第三者機関の体制を整備する。
- なお、制度改正に当たっては、国境を越えたデータの流通を阻害することがないよう、国際的に調和のとれた我が国として最適な制度とすることを目指す。

パーソナルデータの利活用に関する制度改正について 2



パーソナルデータの利活用に関する制度改正について 3

基本的な枠組み

①本人同意に代わる一定条件のもと、データを利活用可能とする枠組みの導入

- 法律上原則として本人の同意が求められる第三者提供等について、本人同意に代わるデータ利活用の枠組みとして、提供側で「個人の特定性を低減したデータ」への加工と、受領側で特定の個人を識別することを禁止するなどの適正な取扱いを規定。
- 医療情報等のように適切な取扱いが求められつつ、本人の利益・公益に資するために一層の利活用が期待されている情報も多いことから、萎縮効果が発生しないよう、適切な保護と利活用を推進。

②基本的な制度の枠組みとこれを補完する民間の自主的な取組の活用

- 事業者が利活用に躊躇しないよう、「個人情報」の範囲を明確化し、本人の権利利益の侵害が生じることのないようその取扱いを規定。
- 技術の進展に迅速に対応することができる制度の枠組みとする。
- パーソナルデータの利活用の促進と個人情報及びプライバシーの保護を両立させるため、マルチステークホルダープロセスの考えを活かし、消費者等も参画する民間主導による自主規制ルールの枠組みを創設。
- 民間団体が、業界の特性に応じた具体的な運用ルール（例：個人の特定性を低減したデータへの加工方法）や、法定されていない事項に関する業界独自のルール（例：情報分析によって生じる可能性のある被害への対応策）を策定し、その認定等実効性の確保に第三者機関が関与する枠組みを構築。

③第三者機関の体制整備等による実効性のある制度執行の確保

- 法定事項や民間における自主的な取組について実効性ある執行を行うため、国際的な整合性も確保しつつ、第三者機関の体制を整備。
- 第三者機関については、特定個人情報保護委員会を改組し、パーソナルデータの保護及び利活用をバランスよく推進することを目的とする委員会を設置。
- 第三者機関は、現在個人情報取扱事業者に対して主務大臣が有している機能・権限に加え、立入検査等の機能・権限を有し、また、民間の自主規制ルールの認定等及びパーソナルデータの越境移転に関して相手当事国が認めるプライバシー保護水準との適合性を認証する民間団体の認定・監督等を実施。
- 事業者が法令違反に当たる行為をした場合等の手段として、現行の開示等の求めについて、請求権に関する規律を定める。

創造的IT人材育成方針の概要

「世界最先端IT国家創造宣言」における人材育成・教育分野の位置付けを踏まえ、
府省横断的に取り組むための方針として、「創造的IT人材育成方針」を策定する。

本方針が目指すもの （目標）

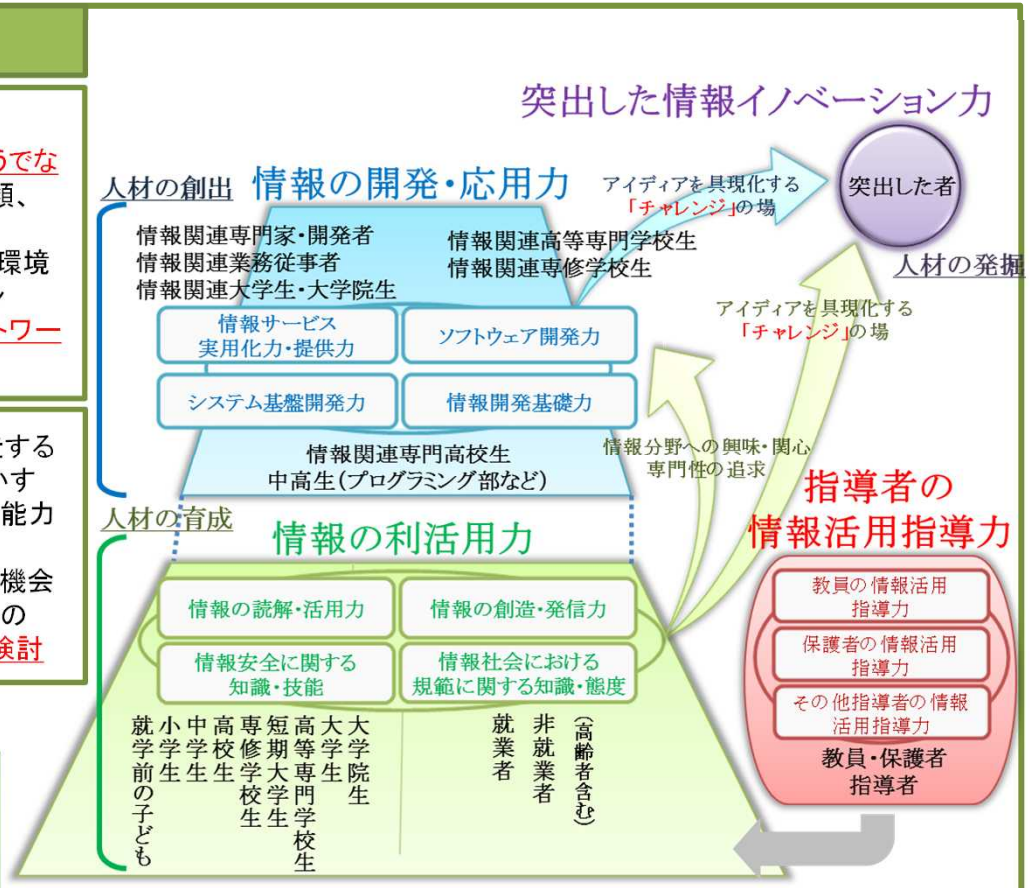
「国民全体のIT利活用能力の底上げ」と「我が国の経済発展に寄与する高度なIT人材の創出」によって、さらなる経済成長の基盤を構築し、2020年までに「世界最高水準のIT利活用社会」の実現を目指す。

目標達成に向けた本方針のアプローチ

ITの利便性を享受して生活できる社会の構築と環境の整備 （国民全体のITリテラシー向上）	● 学校現場の教育等の従来のアプローチに加え、就学前の子どもから高齢者、ITを得意とする人とそうでない人、教育・指導する人等を意識し、国民全体を分類、各層に求められる能力項目を設定 ● 学びの充実や安全・安心な利活用を導くための環境として、指導者の情報活用指導力向上とクラウドコンピューティングサービスやMOOC活用等の情報ネットワーク基盤構築、学習コンテンツの整備について検討
日本のIT社会をリードし、世界にも通用するIT人材の創出 （高度IT人材の育成）	● 高度IT人材をITの枠を超えイノベーションを創造する「IT利活用社会をけん引する人材」とITを業務に活かす「IT利活用社会を支える人材」に分類し、求められる能力項目を設定 ● 実践的な人材育成のための産学連携や成長の機会につながる競技会等のイベントといった“チャレンジの場”を提供、高度IT人材の発掘、育成、成長支援を検討

人材育成分科会

本方針に基づき
- 関係府省が取り組むべき具体的活動計画を検討
- PDCAを意識したフォローアップ
（KPI達成状況評価、計画見直し等）



本方針における対象者と求められる能力の全体像

「サイバーセキュリティ戦略」（平成25年6月情報セキュリティ政策会議）における主な取組み

	政府機関・独立行政法人等	重要インフラ事業者	企業・一般個人
「強靱な」サイバー空間（守り強化）	●機微情報を守るためのリスク評価手法の確立【2014年6月】・統一基準の見直し【同年5月】 ●GSOCの強化、CYMAT・CSIRTとの連携による 的確・迅速な対応 ●対処訓練の実施（3・18（サイバー）の日）、警察・自衛隊等の関係機関の役割整理 ●SNS・グループメールを含む新サービスに伴う新たな脅威への対応【2014年5月】	●重要インフラの範囲拡大や安全基準見直し等行動計画の見直し【2014年5月】 ●政府機関やシステムベンダー等との情報共有の強化 ●事業継続確保のための分野横断的な演習 ●重要インフラで利用される制御機器等を国際標準に則って評価・認証するための基盤構築	●スマートフォン不正アプリへの対応 ●情報セキュリティ月間・「サイバーセキュリティの日」創設【毎年2月】 ●普及啓発プログラム（2011年情報セキュリティ政策会議）の改訂【2014年7月】 ●税制など中小企業のセキュリティ投資の促進 ●ISP等による個人への感染に関する注意喚起などIT 関係事業者の取組 ●ログ保存の在り方検討などサイバー犯罪の事後追跡可能性の確保
「活力ある」サイバー空間（基礎体力）	●人材育成プログラム（2011年情報セキュリティ政策会議）の改訂【2014年5月】 ●研究開発戦略（2011年情報セキュリティ政策会議）の見直し【2014年7月】		
「世界を率先する」サイバー空間（国際戦略）	●日ASEAN【2009年～：日ASEAN政策会議[注1]（2014年10月・東京）】等 ●日米【2013年～：日米サイバー対話（2014年4月・ワシントンDC）】等 ●日英【2012年～：日英サイバー協議】 ●日印【2012年～：日印サイバー協議】 ●日EU、日仏、日イスラエル、日エストニア、日豪、日露…【今後、二国間協議を開催見込み】 ●サイバー空間の国際規範づくり等に関する会議【2011年～：次回（2015年4月・オランダ・ハーグ）】 ●IWWN[注2]（2014年5月・東京） ●MERIDIAN[注3]（2014年11月・東京）		●共同意識啓発活動【毎年10月】
組織体制	●国際戦略の策定【2013年10月】 ●NISCの機能強化（サイバーセキュリティセンター（仮称）への改組：**2015年度目途**）		・GSOCの強化 ・GSOC保有情報の重要インフラ事業者との共有の仕組み ・必要な人材等の在り方　等

〈注１〉 日・ASEAN情報セキュリティ政策会議。各国局長級が参加。
〈注２〉 サイバー空間の脆弱性、脅威、攻撃に関する国際的取組の促進。米・独・英・日等の政府機関、CERTが参加。
〈注３〉 重要インフラ防護等のベストプラクティス共有や国際連携等に関する意見交換。米・英・独・日等の政府機関が参加。

「情報セキュリティ研究開発戦略（改定版）」の概要について

サイバーセキュリティ戦略（2013年6月策定） において示された
○ サイバー攻撃の検知・防御能力の向上
○ 制御システム、ICチップなど社会システム等を保護するためのセキュリティ技術の確立
○ ビッグデータ（パーソナルデータ等）利活用等の新サービスのための技術開発　等

を推進する観点から、**「情報セキュリティ研究開発戦略」を改定**

情報セキュリティ研究開発の推進方針

1. **サイバー攻撃の検知・防御能力の向上**
   - 分散しているサイバー攻撃情報等の共有のための組織等の連携強化
   - 研究者等へ政府の有するサイバー攻撃の検体等の提供等を検討
2. **社会システム等を防護するためのセキュリティ技術の強化**
   - 制御システム等のセキュリティ技術の国際標準化・認証制度等を推進
3. **産業活性化につながる新サービス等におけるセキュリティ研究開発**
   - 今後発展が期待されるIT利用分野で上流工程からセキュリティ品質の組込を推進
4. **情報セキュリティのコア技術の保持**
   - 暗号等のコア技術の保持は、我が国の新規産業創出や安全保障等の観点から重要であり維持・強化
5. **国際連携による研究開発の強化**
   - 各国が「強み」を有する技術を組合せ発展させるため、研究者受入等国際連携を推進

研究開発の効果・成果を高めるための方策等

1. 研究成果の社会還元の推進
2. 必要な研究開発リソースの確保と柔軟性確保
3. 情報セキュリティ技術と社会科学など他分野との融合

情報セキュリティ研究開発における重要分野

（※　左記の観点を踏まえ、重要分野を整理）

（1）情報通信システム全体のセキュリティの向上
サイバー攻撃の検知、認証、次世代ネットワーク　等
（2）ハード・ソフトウェアセキュリティの向上
制御システム、デバイス、ソフトウェアの安全性確保　等
（3）個人情報等の安全性の高い管理の実現
プライバシー保護、パーソナルデータ利活用　等
（4）研究開発の促進基盤の確立と理論の体系化
理論体系化、調査研究、標準化、評価、暗号技術　等
（5）発展分野でのセキュリティ研究開発
医療健康、農業、次世代インフラ、ビッグデータ、自動車のネットワーク接続　等