ビッグデータ社会の課題
ーセキュリティを中心にー

2018年11月14日
才所敏明 (株)IT企画
（中央大学研究開発機構）
toshiaki.saisho@advanced-it.co.jp
http://www.advanced-it.co.jp/
https://www.facebook.com/toshiaki.saisho

 1

自己紹介

1970年　東芝入社

1970年4月～1994年12月　東芝本社・情報システム部門
社内計算機利用環境企画・構築・活用指導・支援

1995年1月～2007年9月　東芝・セキュリティ技術研究開発部門
情報セキュリティ研究開発企画・推進、事業支援

2007年10月　（株）IT企画設立
事業支援活動（企業の顧問・相談役）
大学教育活動（九大・慶応にて講義・講演）
研究開発活動（IT企画・中央大学研究開発機構）
サイバーセキュリティ、バイオメトリクス、
ビッグデータ、IoT、FinTech（仮想通貨、ブロックチェーン）

 2

本日の内容

（1）はじめに

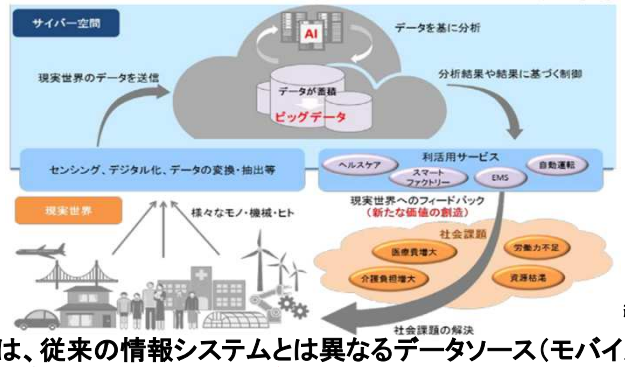
（2）ビッグデータ活用推進上の課題

（3）ビッグデータを構成する
サブシステムのセキュリティ課題

（4）おわりに

 3

（1）はじめに
ビッグデータ社会への期待



（平成28年
総務省資料より）

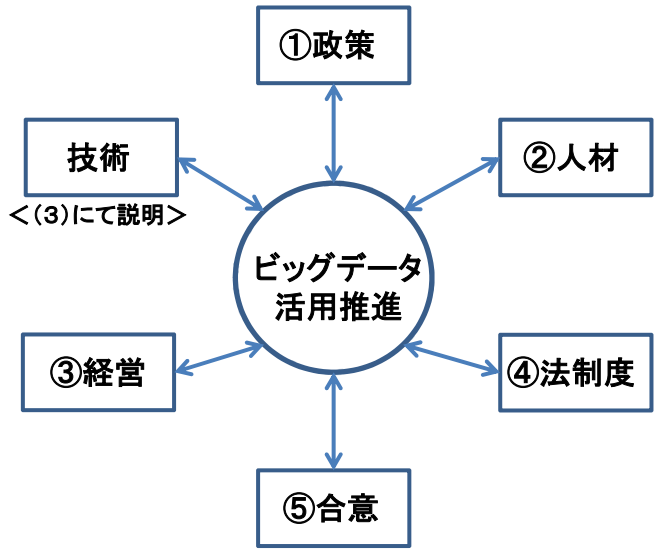
ビッグデータは、従来の情報システムとは異なるデータソース（モバイルデバイスやIoT等）からのデータとの結合による**データフュージョンの発生**や、発展する人工知能技術（AI）による**データの高度利用**を可能とし、社会での活用が期待されている。

ビッグデータ、IoT、AIは相互に連携しながら発展をつづけ、**データ・ドリブン（駆動型・主導）社会、ビッグデータ社会**へと発展することになろう。

しかし、ビッグデータの具体的な活用推進には、留意・克服すべき課題も多い。
本日は、セキュリティ課題を中心に紹介したい。

 4

（2）ビッグデータ活用推進上の課題



①ビッグデータ社会に向けた政策

「日本再興戦略2016」（平成28年6月閣議決定）

“今後の生産性革命を主導する最大の鍵は、IoT（Internet of Things）、ビッグデータ、人工知能、ロボット・センサーの技術的ブレークスルーを活用する「第４次産業革命」である”

名目GDP600 兆円に向けた「官民戦略プロジェクト 10」の一つとして、**新たな有望成長市場の創出のための「第４次産業革命（IoT・ビッグデータ・人工知能）」の推進**を掲げている。**＜付加価値創出：30兆円(2020)＞**

「世界最先端IT国家創造宣言・官民データ活用推進基本計画」

（平成29年5月閣議決定）

「官民データ利活用社会」～データがヒトを豊かにする社会～モデルを世界に先駆けて構築を目指し、「我が国の置かれた諸状況を踏まえたデータ利活用による新たなライフスタイルの提案」、**「官民データの利活用に向けた環境整備」等の施策**を掲げている。

「未来投資戦略2017」（平成29年6月閣議決定）

「未来投資戦略2017」においても、**Society 5.0** に向けた課題の一つとして、**「データ利活用基盤の構築、徹底したデータ利活用に向けた制度整備」**を掲げている。

「第5期科学技術基本計画」（平成28年1月閣議決定）

“超スマート社会サービスプラットフォームの構築に必要となる基盤技術、すなわち**サイバー空間における情報の流通・処理・蓄積に関する技術は**、我が国が世界に先駆けて超スマート社会を形成し、ビッグデータ等から**付加価値を生み出していく上で不可欠な技術**である”

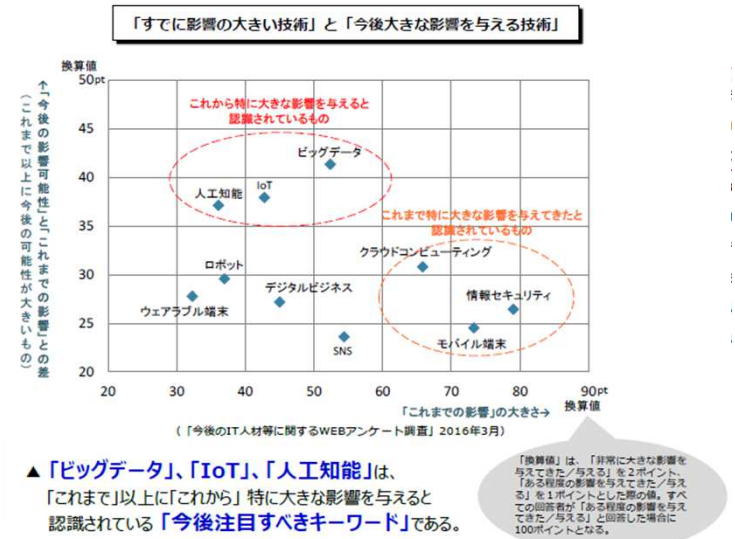
とし、非構造データを含む多種多様で大規模なデータから知識・価値を導出する「ビッグデータ解析技術」の強化を図る、としている。

（Society5.0の提唱：ICTを最大限に活用し、サイバー空間とフィジカル空間（現実世界）とを融合させた取組により、人々に豊かさをもたらす「超スマート社会」を未来社会の姿として共有し、その実現に向けた一連の取組を更に深化させつつ「Society 5.0」として強力に推進し、世界に先駆けて超スマート社会を実現していく。）

「科学技術イノベーション総合戦略2017」（平成29年6月閣議決定）

新たな経済社会である Society 5.0 を実現していくためには、新たな価値創出を容易とするプラットフォームを構築することが重要とし、取り組む必要がある施策として「新たな価値やサービスの創出の基となるデータベースの構築と利活用」、「プラットフォームを支える基盤技術の強化」などを掲げ、“特に、**AI技術、IoTシステム構築技術、ビッグデータ解析技術等のいわゆるAI関連技術は Society 5.0 を実現する鍵**であり、世界の先を見据えた水準に昇華させ、更に社会実装を迅速に推進することが肝要である”としている。

②人材



IT人材の最新動向と将来推計に関する調査結果（2016年6月METI資料より）

データサイエンティスト育成の遅れ

2012年のガートナー報告：当時、日本には千人程度のデータサイエンティスト。将来、日本では25万人程度、不足する。

2014年の日本学術会議報告：
欧米やアジア諸国では統計学などのビッグデータに関連する教育組織や学位授与数が急速に増加。
諸外国がデータサイエンティストを急速に増加させている中で、我が国だけが逆に減少。
今後の我が国の科学技術研究発展及び産業におけるイノベーションにむけて重大な問題。
早急な対応が必要。

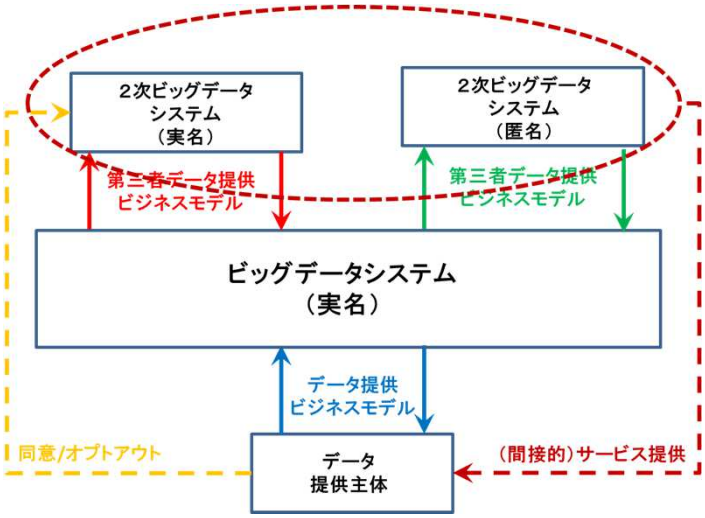
データ分析専攻の学生、日本は育成に遅れ（データ分析の訓練を受けた大学卒業生の数）

米国	2万4730人
中国	1万7410
インド	1万3270
ロシア	1万2300
ブラジル	1万　90
ポーランド	8780
英国	8340
フランス	7770
ルーマニア	4970
イタリア	4900
日本	3400

科学技術白書（2016年文部科学省）より

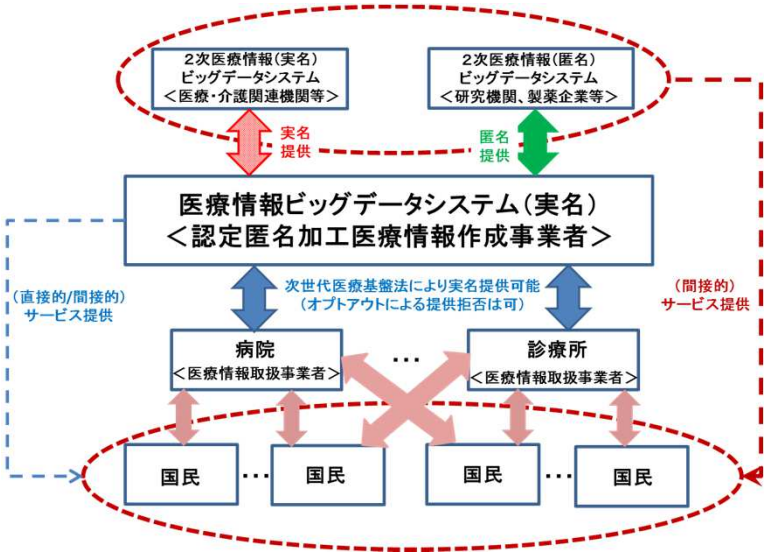
2018年9月28日「政府、AIの総合戦略策定へ」
2019年4月に「AI戦略パッケージ」を取りまとめる。
「教育改革」で検討される予定の項目
大学修了者のレベルを認証する仕組みの整備
数理・データサイエンス教育を3年以内に全大学生に必修化

③経営



ビッグデータエコシステムの構築

医療分野における
ビッグデータエコシステム例



 11

④法制度

(1)ビッグデータにおける不適切なデータ利用を防ぐための法制度
(個人情報・パーソナルデータの適切な取扱い)

＊改正個人情報保護法(平成29年5月30日施行)
個人情報の定義の明確化(個人識別符号の定義)
公的な番号(マイナンバー、免許証番号等)
身体的特徴を示す符号(顔、虹彩、指紋、DNA等)
慎重な取扱いを要する個人情報を定義
要配慮個人情報(病歴・犯罪歴に関するもの)
原則として本人の同意をとることを義務化

 12

（2）ビッグデータ活用促進を促す法制度

＊改正個人情報保護法（平成29年5月30日施行）
個人情報の事前の本人の同意を得なくとも
オプトアウト方式による第三者提供が可能
匿名加工情報の利活用に関する規定を新設
個人を識別できないように個人情報を加工し、
当該個人情報を復元できないようにした情報
第三者提供に本人の同意、オプトアウトの仕組みは不要

＊次世代医療基盤法（平成29年4月成立）
要配慮個人情報に該当する医療情報も
認定匿名加工医療情報作成事業者に対しては
オプトアウト方式により第三者提供可能

 13

（3）データの独占・寡占の弊害を防ぐ法制度
（自由な競争環境の確保）
データが大きな価値を持つようになりデータの独占や寡占が
企業の競争を制限することにもなりかねないことが懸念

＊OECD（2016年10月）：
「Big Data：Bringing Competition Policy to the Digital Era」

＊公正取引委員会（2017年6月）：
「データと競争政策に関する検討会報告書」
＝＞市場での支配的立場を使ってのデータ収集や
不当なデータの囲い込みは、独占禁止法の適用を検討

 14

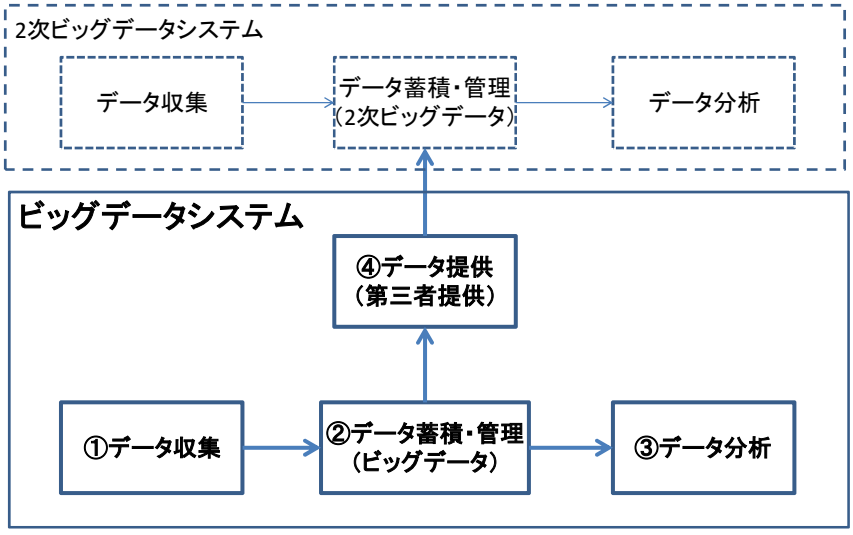
⑤合意（国民の理解）

（1）本人への直接的なサービスのためのデータ提供
　　データ提供主体へのインセンティブを確保し、
　　ビッグデータエコシステムを確保すること
　　＝＞個人を支えるビッグデータ

（2）社会を構成する国民の一人としてのデータ提供
　　国民生活を支える社会インフラの維持・高度化
　　国民の健康増進や医療・医薬の
　　改良・高度化のための基礎研究開発
　　＝＞社会を支えるビッグデータ（公共財？）

 15

（3）ビッグデータを構成する サブシステムのセキュリティ課題



 16

①データ収集サブシステム

（1）データ量の爆発

（2）データ構造の多様化

（3）データの品質確認・調整

（4）データの真正性確保（誤データ、悪意のあるデータの混入検知）
＜＝送信機器および送信データの認証（暗号技術）

（5）データの秘匿性確保（収集データの価値保護）
＜＝送信データの秘匿（暗号技術）

（6）個人情報・要配慮個人情報の適正取得
個人情報の取得：利用目的を、
本人に通知または公表することが必要
要配慮個人情報の取得：本人の同意が必要

＜改正個人情報保護法：平成29年5月30日施行＞

②データ蓄積・管理サブシステム

（1）多様な構造の大量なデータの蓄積・管理

（2）データの維持・保全
（データの破壊や改ざん、ランサムウェア等への対策）
＜＝アクセス者の認証（暗号技術）、バックアップ

（3）データの漏洩防止（バックアップデータからの漏洩防止も含め）
＜＝アクセス者の認証（暗号技術）、
＜＝暗号化によるデータ保護（暗号技術）
＜＝分散保管によるデータ保護（秘密分散技術）

（4）保有個人データに対する
本人の要求（開示、訂正、利用停止等）への対応

③データ分析サブシステム

（1）統計学に基づく分析（＝＞深刻な人材不足の問題）

（2）人工知能・機械学習・深層学習による分析
　　一般に分析結果の説明が困難
　　（根拠導出・提示が可能な分析技術の研究開発が必要）

（3）分析過程のデータ保護（セキュア分析）
　　＜＝暗号化されているデータの保護（暗号化状態処理）
　　＜＝秘密分散されているデータの保護（秘密分散状態処理）

（4）分析結果の利用に関する責任の所在
　　責任の所在に関するエンティティ間の事前の合意が必須
　　（データ収集主体、分析機能提供主体、分析者、利用者）

 19

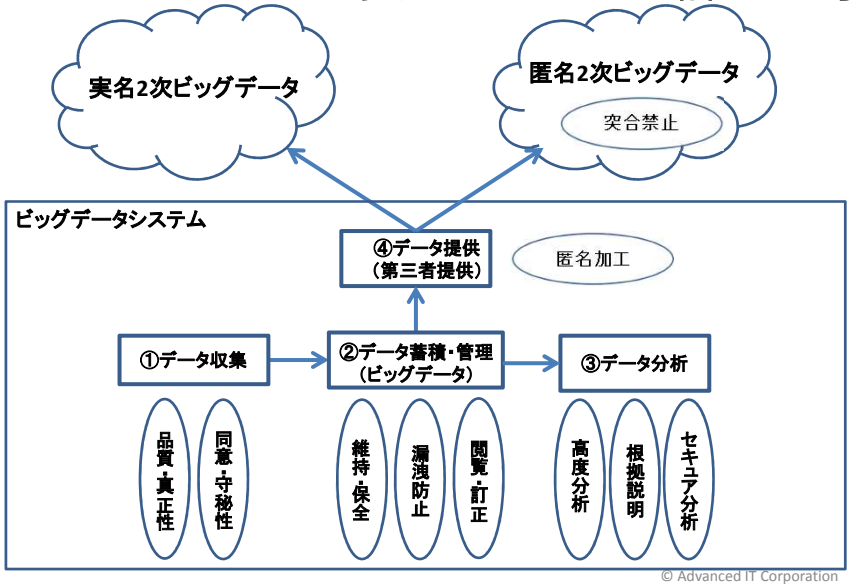
④データ提供（第三者提供）サブシステム

（1）実名のまま提供
　　個人情報：原則本人の同意による提供
　　オプトアウトによる提供も可
　　要配慮個人情報：本人の同意による提供
　　（オプトアウトによる提供は認められていない）

（2）匿名化し提供
　　匿名加工情報
　　個人を識別できない/個人情報を復元できない
　　本人の同意は不要
　　匿名加工情報に含まれる情報項目の公表

 20

ビッグデータを構成する サブシステムの主要セキュリティ課題一覧



 21

期待されるセキュリティ技術 暗号技術、暗号化状態処理

(1)暗号技術

共通鍵暗号:DES(1976)、AES(2001)、NESSIE(2003)、
CRYPTREC(2003)

公開鍵暗号:DH鍵共有(1976)、RSA(1978)、楕円曲線(1985)

(2)最近の動向(研究開発、応用)

IoT向け軽量暗号:CRYPTRECにて評価、
暗号技術ガイドライン(軽量暗号)に結果記載

耐量子計算機(PQC)暗号:NISTにて標準化中
{LOTUS(NICT)、Giophantus(東芝、他)等、日本からも応募}

暗号化状態処理:基礎研究・実用化研究が中心だが商品化も。
{NTT、NEC、産総研が秘密計算(統計分析)を実用化}

 22

期待されるセキュリティ技術
秘密分散技術、秘密分散状態処理

（1）秘密分散技術

しきい値方式：Blakley/Shamir考案（1979）、
ランプ型しきい値分散法（1985、山本）

AONT方式：Rivest考案（1997）、CTRT-AONT（2000、Desai）

（2）最近の動向（研究開発、応用）

しきい値方式：ISOが秘密分散技術の標準規格
ISO/IEC 19592-2:2017を発行
{5つの秘密分散方式が採択され、NTT独自方式も採択}

AONT方式：実用的パッケージ製品が市場へ
{ZENMU-AONT（CTRT-AONTの改良版）}

秘密分散状態処理：基礎研究・実用化研究が中心だが商品化も。
{秘密計算システム 算師®（NTT）等}

 23

（4）おわりに

①我が国だけでなく、各国がビッグデータ社会を目指し、研究開発・技術開発・社会実装を展開中。

②ビッグデータ活用推進にあたっては、多くの留意すべき項目・課題もあるが、慎重にしかし果敢に取り組む必要がある。

③ビッグデータシステム構築・運用上においても、更なる研究開発が必要な課題も多いが、実用化が可能な、実用化が間近な最新の研究開発成果も多い。

④課題の存在は、ビジネスチャンスでもある。今回の紹介内容が、皆さんの事業活動にお役にたてば幸いである。

 24

終

本発表は、以下のこれまでの研究成果・調査結果をベースに、
最近の状況を加味し整理したものである。

＊SCIS2018発表論文「ビッグデータの社会活用推進上の課題に関する考察」:
http://advanced-it.co.jp/2016_wp/wp-content/pdf/20180124SCIS2018paper.pdf

＊調査報告書「ビッグデータの利活用に関する現状・動向・課題」:
http://advanced-it.co.jp/2016_wp/wp-content/pdf/20180401_bigdata.pdf

