情報インテグレーションについて

伊藤　博文[†]（愛知大学法科大学院）

要旨

情報が氾濫しその重要性が増す社会の中で，これまでとは異なる情報のインテグレーション（集約）が行われつつある。個人情報保護やプライバシーといった考え方から守られてきた情報がビッグデータ解析やオープンソース調査という手法で，秘匿化が骨抜きにされ個人レベルでは保護し得ない状況となり，あらたな望ましい情報管理のあり方が必要とされるようになる。これについての問題点と対応手法について考察する。

キーワード：ビッグデータ　情報インテグレーション　プライバシー　オープンソース調査

1. はじめに

本稿の目的は，情報インテグレーション（II: Information Integration）[2]にかかわる問題点を考察することにある。情報インテグレーションとは，言葉通りに情報の集約であるが，単にビッグデータ解析から生み出される新たな集約された情報に留まらず，元データとは異質の情報を生み出す処理操作を指し，単なる集約という言葉だけでは表せない意味を持つ。この処理操作から生み出される情報が社会的に有用であるのは当然であるが，我々の社会における情報のあり方を根本から覆す恐れのあるものであり，慎重に扱うことを議論する必要がある。この意味で，情報インテグレーションの持つ問題点を検討することが喫緊の課題である。

2. 情報インテグレーションとは

情報インテグレーションを考えるにあたり，まずは2つの事例から考えていきたい。

[†] 愛知大学法科大学院教授。以下のメールアドレスに忌憚なき意見や批判を送付していただければ幸いである。hirofumi@lawschool.aichi-u.ac.jp。今後，本稿の改訂が必要な場合は，改訂版をhttp://cals.aichi-u.ac.jp/project/PN0160.htmlにてPDFファイルで公開する予定であり適宜参照いただければ幸甚である。また，本稿引用文中URLの最終アクセス確認日は2019年11月27日である。

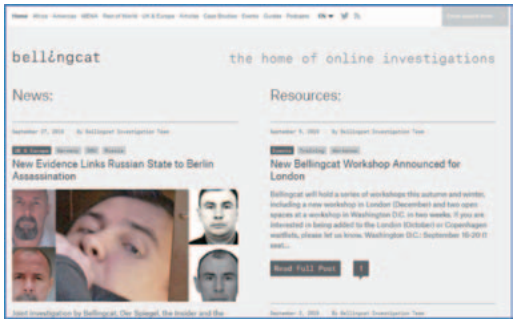
[2] https://en.wikipedia.org/wiki/Information_integration 参照。

2.1. オープンソース調査

インターネット上で繰り広げられるCyber空間では，さまざまな情報発信が行われているが，いわゆる「ニュース」という事実を伝えるべき報道情報の中に偽物（Fake）とされる情報が蔓延した状態となり，事実報道の真偽を誰もが判定できない状態に陥り，情報が錯綜し社会問題化してきている。

そこで，情報処理技術に長けた市井の人達が，オープンソースの情報を集約して，真相を突き止めるという活動が行われている。

2014年ウクライナで起きたマレーシア航空17便撃墜事件[3]の真相は，ウクライナとロシアの間で互いに相手が撃墜を行ったと非難し合い，真相はどの報道メディアも突き止めることができなかった。BELLINGCAT（猫に鈴をつけるの意）という名のインターネット上で活動するグループがある。エリオット・ヒギンス氏が率いる集団で，画像分析や音声解析，位置情報の特定などに精通したメンバーとボランティアから構成されている。Google Earth[4]の衛星画像写真が示す位置情報，Google Street view[5]の街頭の映像が示すミサイル自走発射機の映像，戦地に赴く息子を心配する母親のSNS上での日常での対話など，誰もがアクセスできるオープンソース情報を地道な情報処理操作で一元集約することにより，撃墜したのはロシア軍であることを突きとめたのである。



BellingCat
https://www.bellingcat.com

すなわち，既にこの世界中に散在するオープンソース情報を1つの目的でインテグレーションを行うことにより，誰もが知り得なかった，また隠し通されたままの情報を明るみに出すことができることを証明しているのである。事実は存在しその事実から漏れ発せられるオープンソース情報が自由にアクセスできる環境であれば，誰もが情報インテグレーションを行い，求める情報を生み出すことができる。

[3] https://ja.wikipedia.org/wiki/マレーシア航空17便撃墜事件
[4] https://www.google.co.jp/earth/
[5] https://www.google.co.jp/intl/ja/streetview/

2.2. 匿名からの個人特定

Luc Rocher氏らの研究[6]に依れば，ビッグデータなどで広く活用される匿名化された大量のデータには安全性に問題があるとされる。この研究結果では，プライバシー保護のためにデータが匿名化されていても，性別，人種，生年月日，郵便番号，住宅ローン，学歴，結婚歴，車所有の状態，職業，市民権の状態といった複数の断片的な情報を手がかりに，近時の統計学や機械学習の計算手法を駆使すれば，高い確率で個人の特定が可能であったとしている。

さまざまな分野で利用されるビッグデータ分析の基となる匿名化された個人データは，提供前に個人を識別されそうなデータ要素を取り除いて匿名データ化され汎用データとして利用されるが，専門知識を持った者が統計学や機械学習の計算手法を駆使すれば，地域住民の99.98％の個人が特定可能であることを指摘している。

すなわち，匿名化作業はビッグデータ時代において意味のないものとされてしまうことを指摘しているのである。

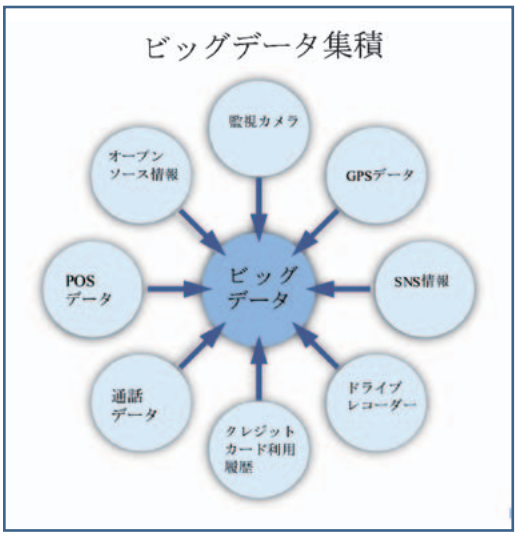


Figure 1 ビッグデータの集積

2.3. ビッグデータの情報源

高度の監視社会といわれる今日において，さまざまな形態で個人にかかわる情報が収集されつつある。

第1は，不同意に情報収集されるデータ群である。本人に情報収集されていることの同意を全く取らずに一方的に行われる情報収集方法である。

まずは，街中に設置してある多数の防犯カメラ画像データである。警察庁によれば「防犯カメラ画像は，被疑者の特定や犯行の立証に有効であることから，事件関係者の足取りの確認，防犯カメラ画

[6] Luc Rocher, Julien M. Hendrickx & Yves-Alexandre de Montjoye, *Estimating the success of re-identifications in incomplete datasets using generative models*, NATURE COMMUNICATIONS (2019), https://www.nature.com/articles/s41467-019-10933-3.pdf.「ビッグデータ，匿名化でも高確率で個人特定　海外で指摘」2019年8月11日朝日新聞朝刊，https://www.asahi.com/articles/photo/AS20190810002696.html。

像を公開しての追跡捜査等，警察捜査における様々な場面で活用されている。防犯カメラ画像の分析結果から被疑者の検挙に結び付いた事件の中には，被害者と全く面識がない被疑者による偶発的な犯行によるものもあり，防犯カメラ画像は，今や警察捜査に欠かせないものとなっている。」[7]としている。

さらに，高速道路上の自動料金収受システム（ETC）などの記録[8]，検疫目的で設置されている空港のサーモグラフィーも，本人の同意のないまま体温情報が収集・記録されている。空港の出入国管理では，強制的に顔写真と指紋が採取される。その利用目的は自明のこととして，本人に口頭で情報収集時に説明されることはない。拒否すれば，出入国できないだけである。防犯カメラ型のセンサーで人工知能を使った顔認証は，防犯カメラと同じく，その場にいる者全員の情報を取得しているが同意は得ていない。Webアクセス時に発生する情報（クッキー（cookie），ウェブビーコン（web beacon））[9]，広告用識別子などの技術を使用して取得したアクセス情報も実質的に同意を得ずに収集され，目的外利用の恐れは高い。

そしてIoT（Internet of Things）[10]がもたらすデータ管理である。冷蔵庫内に残された野菜や牛乳といった食材の消費期限がインターネット経由で遠隔地からわかり今日購入すべき食材を教えてくれ，外出先から自宅の電灯・クーラーといった家電のOn/Offが自在にできるとして利用される技術であるが，使われた機器操作の情報データも記録・一元集約可能である。

第2は，同意型の情報収集である。

携帯電話の通話履歴は，プライバシー・ポリシー[11]により保護され誰でも見られる情報ではないが，今や警察捜査には欠かせない情報データとなっている。管理主体は各携帯電話会社であり，恣意的な情報管理が行われても誰も知らないままで済まされてしまう可能性がある。

---

[7] 特集：変容する捜査環境と警察の取組　https://www.npa.go.jp/hakusyo/h26/honbun/html/qf310000.html。

[8] 有料道路自動料金収受システムにおける個人情報の保護に関する指針　https://www.its-tea.or.jp/library/law/guideline.html。

[9] Cookieの利用規制については，就職情報サイト「リクナビ」を運営するリクルートキャリア社が就職活動中の学生のサイト閲覧履歴などを基に内定辞退の指標を採用企業に提供していた問題が記憶に新しい。この問題を受けて，個人情報保護委員会が，個人情報保護法改正に取り組むこととなっている。「『クッキー』利用に法規制　リクナビ問題受け改正へ」日本経済新聞社2019年11月26日記事，https://www.nikkei.com/article/DGXMZO52606310W9A121C1000000/参照。

[10] IoTは，「モノのインターネット」とも言われ，これを実装したものの一つがコネクティッド技術である。https://ja.wikipedia.org/wiki/モノのインターネット　参照。

[11] たとえば，https://www.kddi.com/corporate/kddi/public/privacy/exhibit2/　参照。

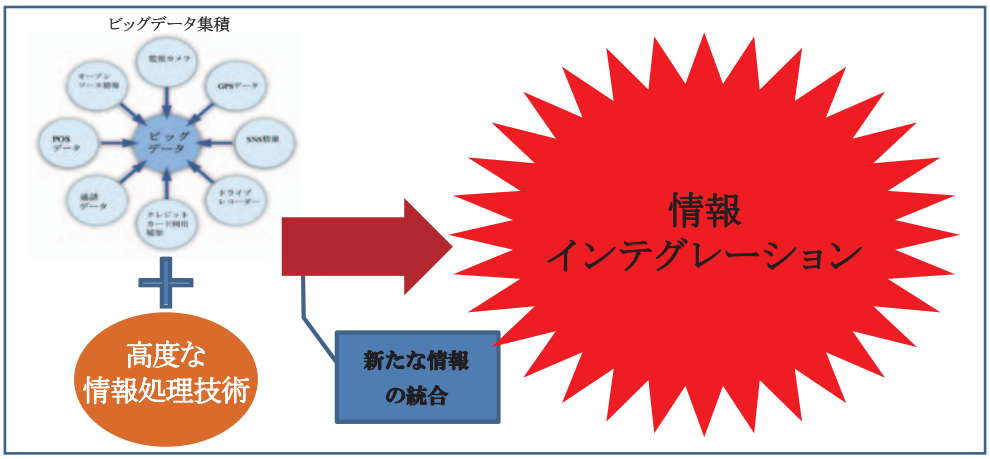


Figure 2　情報インテグレーションの流れ

生体認証が求める個人情報は，目的外流用されないという信頼関係に基づきやり取りされているが，生体認証が求める，虹彩・指紋・静脈・行動様式などの情報がどのように処理されているかを検証する術は無い。医療機関の持つ電子カルテ上の病歴・既往症などの個人情報，調剤薬局の持つ薬事情報，社会保険会社の持つ顧客の治療情報，など同様である。

種々の個人認証操作がもたらすデータの集約も同様である。コンビニのATMからお金を引き出したときの機器操作記録，銀行のATMにおける機器操作データ，パスポートによる出入国管理データ，航空券の購入履歴情報，運転免許証に記載される住所・本籍地・生年月日，住民基本台帳による住民管理情報，学校における学業成績簿，卒業アルバム上の個人写真や氏名，学級の連絡網一覧表が示す住所・電話番号，クレジットカード利用履歴，等々である。

まさに，高度情報化社会を超えた超高度情報化社会が到来しているのである。ゆりかごから墓場まで，人が生きている間に生み出す情報は全てインターネットを経由してビッグデータの中に入ることになる。

こうした情報収集は高度化し，それに伴うデータ集約は不可避であり，問題は誰がそれを適切にコントロールするのかである。

2.4. 情報インテグレーション

こうしたビッグデータとなった情報は，現状は様々な組織や個人が個別に記録保管しており，その手持ちデータの利用可能範囲内で行われるデータマイニング技術を駆使し，データ集約という名の下に，ビッグデータを情報処理して活用

するということが行われてきた。この段階では，情報を集約する時点で特定の意図があるわけではなく，情報加工プロセスを経て統計的な処理を行い，新たなデータを生み出すことに留まる。

これに対し，情報インテグレーションでは，単に文字情報のデータのみならず画像や音声などあらゆる情報を集約して，これまで関連付けられなかったオープンソース情報も含めて全ての情報が一元管理され情報処理され，新たな付加価値の加わった情報を生み出すことに意義がある。

これまでのビッグデータ解析とは次元の異なるインパクトを社会にもたらすものである。

3. プライバシーの果たした役割

情報を護るという観点からいつも引き合いにだされるのは，プライバシーである。そのプライバシーの意義とこれまで果たしてきた役割について考える。

3.1. プライバシーとは

プライバシーとは「他人の干渉を許さない，各個人の私生活上の自由」[12]とされ，「誰もが他人には知られたくない私的な情報を持っている。その個人にとって場合によっては，知られたくない情報となりうる。このような，他人に勝手に踏み込まれたくない個人の私生活上の自由をプライバシー」[13]と一般に定義される。我々の社会生活上の重要な概念の一つである。

次に，プライバシーの発展史である。プライバシーの概念が日本に導入されたのはアメリカからであり，アメリカにおいてプライバシー権が認められるようになったのは，1890年，ウォーレン（Samuel D. Warren）とブランダイス（Louis D. Brandeis）が連名で，「The Right to Privacy」（プライバシーの権利）と題する論文[14]を掲載したことに端を発する。当時，アメリカはイエロージャーナリズムが横行する時代であり，目先の購読者数獲得のため人の私生活を覗き見たり秘密を暴いたりする取材報道には社会的にも批判が加えられようとしていた。そこでプライバシーという概念

[12] 広辞苑第七版。プライバシーについては，伊藤博文「プライバシーと不法行為法」豊橋創造大学短期大学部研究紀要第20号19頁（2003年），*available at* http://cals.aichi-u.ac.jp/products/articles/Privacy&torts.pdf　参照。
[13] 岡本敏雄・山際隆『最新社会と情報　新訂版』実教出版2018年22頁　参照。
[14] Samuel D. Warren and Louis D. Brandeis, *The Right to Privacy: The Implicit Made Explicit*, 4 Harv. L. Rev. 193 (1890).

を創成し，「独りにしておいてもらう権利（the right to be let alone）」が確立されていくのである。アメリカ法において，この論文発表の1890年以前にもプライバシー侵害のような事件を扱った判例等は存在していたが，明確にプライバシー権と判示したものは無かった。1890年以降，ウォーレン・ブランダイス論文に依拠して，後の判例の多くがプライバシー権を確立していくのである。

アメリカでの発端は，マスメディアという急速に発達した情報拡散媒体から個人の情報を護り安寧な生活を維持していくための人格権的権利としてプライバシーを位置づけた。この後，プライバシー保護は，損害賠償制度を基調とする不法行為法に委ねられ，プロッサーの4類型[15]へと結実していく。そして「法と経済学」学派の影響を受け[16]，サーバースペースでのプライバシー保護についてのLawrence Lessigの主唱する財産権論[17]へと流れていくのである[18]。

一方，日本においては，プライバシーは憲法13条が保障する人格権の一部としての幸福追求権に由来するとする。プライバシーは，「私生活をみだりに公開されないという権利」，「独りにしておいてもらう権利」という受動的な側面を協調される定義から，もっと積極的かつ主体的に「自己の情報を自らコントロールし得る権利」として定義する方向へシフトしてきた[19]。

つまり，プライバシーは唯一不変の法概念ではなく時代の変遷につれてその中身を変質させてきている。なかでも，高度情報化社会へと向かった時代では，自己決定権の尊重という考えを徹底することは，プライバシーという個人の持つ情報を自身が積極的にコントロールできるかに焦点が当てられることになる[20]。

3.2. 個人情報とプライバシー

プライバシーと相俟って引き合いに出

---

[15] Prosser and Keeton's Hornbook on *Torts (5th ed.)* at 850 (1984)；望月礼二郎『英米法［新版］』青林書院（1997年）254–256頁。

[16] Guido Calabresi & Douglas Melamed, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, 85 HARV. L. REV. 1089（1972年）。松浦以津子「所有権法ルール，損害賠償法ルール，不可譲な権原ルール：大聖堂の一考察」松浦好治編『不法行為法の新世界』111–172頁，木鐸社（1994年）。

[17] Lawrence Lessig, *CODE VERSION* 2.0, pp. 200–232（2006年）。山形浩生『CODE VERSION 2.0』翔泳社279–324頁（2007年）。

[18] この流れについては，石井夏生利「伝統的プライバシー理論へのインパクト」『AIがつなげる社会 AIネットワーク時代の法・政策』弘文堂（2017年）参照。

[19] 前田達明『民法Ⅵ2（不法行為法）』青林書院新社102頁（1979年）。

[20] 伊藤博文「プライバシーと不法行為法」豊橋創造大学短期大学部研究紀要第20号19頁（2003年），*available at* http://cals.aichi-u.ac.jp/products/articles/Privacy&torts.pdf　22頁参照。

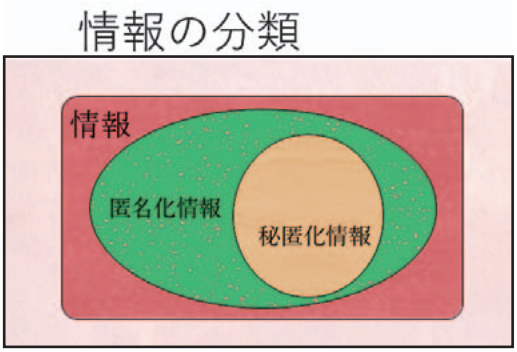


Figure 3　情報の分類図

されるのは，個人情報である。個人情報そのもの定義は，個人情報保護法[21] 2条が規定し，氏名，住所，生年月日，性別，電話番号，学歴，職業など個人に関する情報のうち，生存している個人を特定できる情報としている。特に，氏名，住所，生年月日，性別の4つを基本四情報とし，他の情報と組み合わせることで容易に個人を特定できる情報も個人情報とされる[22]。

個人情報保護法という個別の立法によりプライバシーを守ろうとする意図は，「情報化社会の進展とプライバシー問題の認識」と「個人情報保護法制定の世界的潮流」にあるとする[23]。すなわちプライバシーの具現化を図るために個人情報保護法という法でもって保護範囲を確定して，「個人情報の適正かつ効果的な活用が新たな産業の創出並びに活力ある経済社会及び豊かな国民生活の実現に資するものであることその他の個人情報の有用性に配慮しつつ，個人の権利利益を保護することを目的」[24]としているのである。

3.3. 伝統的プライバシー論の終焉

集団と個という対立構造で人類が社会生活を生きていく中で，個の許容範囲を限定する道具としてプライバシーは働いてきた。人らしい生き方，自由な人生という名の下に機能してきたプライバシー論は，情報インテグレーションにおいては終焉期を迎えつつある。

では，プライバシーという概念はどのような機能を私たちの社会で果たしてきたのであろうか。近代哲学の祖デカルト（René Descartes）のコギト（*Cogito ergo sum*）は「自己と他者」の対立を生み出し，ここにプライバシーの種が蒔かれる。人間社会が成熟し情報伝達量が高まれば，集団から個への干渉が大きくなり，反動として個の存在領域を主張する

[21] 個人情報の保護に関する法律（平成15年法律第57号）。
[22] 岡本敏雄・山際隆『最新社会と情報　新訂版』実教出版2018年22頁。
[23] 基本的人権の保障に関する調査小委員会「衆憲資第28号　知る権利・アクセス権とプライバシー権に関する基礎的資料―情報公開法制・個人情報保護法制を含む―（平成15年5月15日の参考資料）（PDF）」衆議院 pp. 77–78, http://www.shugiin.go.jp/internet/itdb_kenpou.nsf/html/kenpou/chosa/shukenshi028.pdf/$File/shukenshi028.pdf。
[24] 個人情報の保護に関する法律（平成15年法律第57号）第1条（目的）。

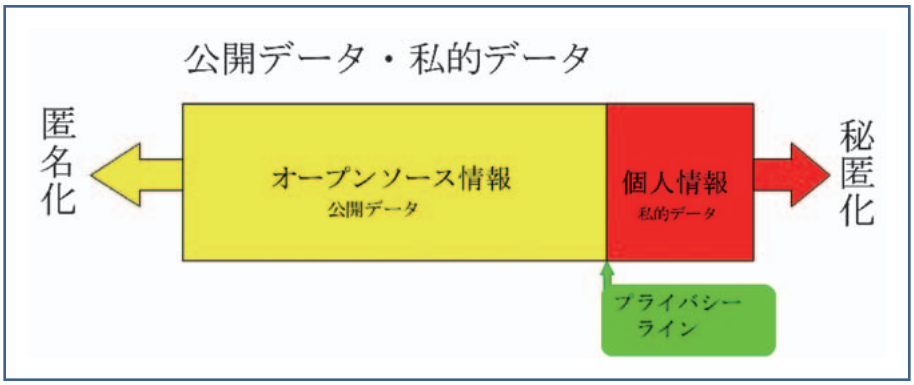


Figure 4　プライバシーライン

必要が出てくる。それは権利による保障であり，情報化社会となると情報の自己コントロール権へと変わる。

しかしながら，超高度情報社会となる現代では，自分で自分の情報をコントロールすることはほぼ不可能である。オプト・イン（Opt In），オプト・アウト（Opt Out）といった情報提供者と情報収集者間の意思表示だけでは，情報管理ができない時代になってきているのである[25]。

4. 新しい情報コントロール

超高度情報社会となる現代において個人で情報をコントロールすることは容易ではない。こうした状況でのコントロール方法について考えてみる。

4.1. ビッグデータ時代のプライバシー

まず，ビッグデータと匿名個人情報との境界線である。AI開発にはビッグデータは不可欠である。ビッグデータは個人情報を匿名化したデータの集合体である。この境界を決める判断基準がプライバシー・ライン（上記Figure 4参照）である。

たとえば，Aさんが週末にデートでイタリア・レストランにて会食をし，スマホ（スマートフォン）の電子決済で代金支払いをしたという情報はどうだろうか。誰が何時・何処で何の代金支払いをしたという情報データは，イタリア・レ

[25] *See*, Ronald Leenes and Silvia De Conca, *Artificial intelligence and privacy – AI enters the house through the Cloud*, Woodrow Barfield, Ugo Pagallo, Research Handbook on the Law of Artificial Intelligence, Edward Elger (2019) p. 280; S.J. Blodgett-Ford, *Future privacy: A real right to privacy for artificial intelligence*, Woodrow Barfield, Ugo Pagallo, Research Handbook on the Law of Artificial Intelligence, Edward Elger (2019) p. 307.

ストラン店の今後の売り上げには大きな情報である。加えて，店内の監視・防犯カメラ，店の向かいにあるマンションの防犯カメラの録画データが一元集約化されることにより，Aさんの個人情報は更に大きな価値を生む。ビッグデータとして欲しいのは，性別，年齢，当日の天気，日付，年収，嗜好，同伴者の数などであろう。これがマーケティング手法により来店予測に繋がり，更に店独自に持つ注文履歴等を合わせれば，材料仕入れにも反映させることが可能である。大きなビジネスチャンスとなる。

この場合，プライバシー上保護されるべき個人情報とされるか否かの境界線は，データ解析の目的により左右されるものであり，一義的には決められない。個人情報とされるものを限定的に列挙してもそれをインテグレーションすることにより，推測が可能となることは既に述べた。

また，知られたくない個人の情報，プライバシーと主唱して保護を求める情報は，主観的に決まる。自分の年齢を対外的にも公にする人もいればひたすら隠そうとする人もいる。しかし，情報データの深層ではそのような情報は公知であり，調べればわかることである。年齢を隠すことによるメリットを求める人にとっては，その場は秘匿できても，戸籍には生年月日が書かれている。プライバシーという判断基準は極めて恣意的なものであり，主観的で恣意的な意思判断を重要視し保護しようとするのもプライバシーである。

4.2. 秘匿と匿名の希釈化

匿名化された情報はビッグデータとして活用されれば有用であるが，プライバシーなどによって保護される情報は利活用されることも日の目を見ること無く消滅すると考えるのがプライバシーの求める帰結である。

これは，情報の全てを知らされず一部のみを知り満足している状態と同じである。まさに「裸の王様」[26]状態である。そして，すべての人類が既に「裸の王様」状態にあるとしたらどうであろうか？つまり，情報インテグレーションが徹底された社会では，あらゆる情報が集約され一元管理されている。もちろん，多元的な管理も可能である。そこでは，存在する情報を個の目で見て見えない情報にす

[26]「裸の王様」については，https://ja.wikipedia.org/wiki/裸の王様　参照。「知らないのは王様本人だけで，王様の臣下と国民はちゃんと知っている。でも王様は満足している。なぜなら自分の情報をきちんと管理していると信じているからだ。」将にこの状態である。情報は常に事実そのものを表象しているのではなく，その事実を人が伝達可能にしたものである。情報は人が作り出すものなのである。

るのがプライバシーである。しかし存在する情報は誰にも隠し通すことはできない。オープンソース情報調査などにより個人情報は丸裸にされてしまうからである。

プライバシーが求める情報の秘匿化は希釈化され薄れ匿名情報との峻別は意味をなさなくなる。

市場経済を前提とする社会では情報は財となり自由に売買され得る。財としての情報の自由な流通というベクトルが大きな力を持つ。ビッグデータ解析による情報分析が新たなビジネスチャンスを生む[27]。だから，プライバシー保護に消極的な国家ほど，多くの有用なビッグデータを持つことができてしまうという現実があり，国家間の不均衡が生じ得る。

情報は存在し続ける。ただそれへのアクセスを否定することで，無い物と扱おうとしているに過ぎない。我々の棲む高度情報社会では，あらゆるところに自分の痕跡を残しながら生きていくことは避けられないのである。

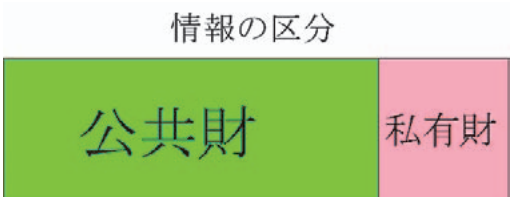


Figure 5　情報の区分

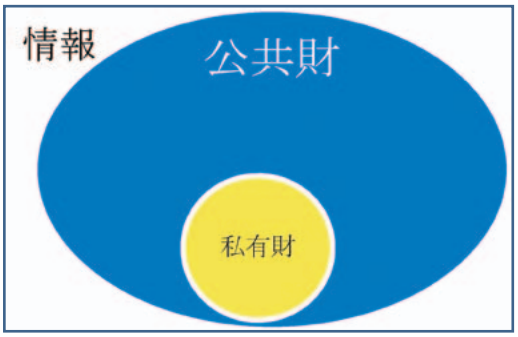


Figure 6　公共財と私有財の包摂関係

4.3. 公共財としての情報

情報は公共財であり，情報は個人の財ではない。公共財である情報の一部を，プライバシーという考え方から秘匿することにより，個人の排他的アクセスを認めているだけなのである。

土地所有制度を例にとろう。国家が国境という名の下にこの地球上に存在する

[27] これは規制に緩やかな国家と厳格な国家下でのAI（人工知能）開発にも言えることである。たとえば，自動車の自動運転技術の開発である。規制の厳しい国家では道路交通法等の規制をたてに，開発段階の自動運転自動車の公道走行を許可しない。また自動運転車が起こす可能性のある事故の法的責任のあり方もAI開発者にとって酷なものとなり，開発意欲を萎縮させる。一方，規制のゆるいもしくは国策的に規制の無い特区などを認めるところでは開発は自ずと進む。人工知能開発は営利企業が主体であり，市場原理が命題となって開発が進むのである。市場は多様な商品としてのAIを出現させ，そのAIの優劣により市場占有が決まり，企業収益が変わる。国家の下での企業活動である限りは，AIは国家の政策に大きく左右されてしまうのである。

土地を囲い込んでいる。これが領土である。この国境内の領土上で，私有財産制度の下に，個人に土地の排他的使用を認める。地球上の陸地という観点から見れば，誰がその一部を支配しているかは瑣末なことである。土地を私的財産制度の下で土地の個人所有を認め，個人に自由に活用させることがその土地自体の価値を最大限化できるという信念の下，こうした制度が近代以降の資本主義社会で行われてきた。しかし，土地の「私的所有 vs. 公共の福祉」という対立構造の下に行われる個と集団の葛藤が，個人所有の範囲を狭める。功利主義的な考えにより，個よりも集団全体が優先された方が価値が上がると考えられるのであれば，個を押さえ全体の利益を優先させることにより，結果として個の利益に繋がるという考えが可能である。これが福祉国家であり，今後も求められるものである。国家が，法制度により国土という財を最大限活用できるように制度運営を行うように，情報も財として全体にとって最も価値の上がる管理手法を考える必要がある。

ビッグデータは，個のデータをより多く集約することによりその価値を増す。個が生み出す情報を個のものとしてプライバシー保護を行い日の目を見させないのは，情報という財を十分に利活用しているとは言えない。オープンソース調査を駆使すればあらゆるプライバシーは存在し得ないはずである。個が生み出す情報は，膨大なセンサーにより日々集約されビッグデータとなっていく。生きていくこと自体が情報発信となり，その情報インテグレーションはもはや誰にも止められないのである。公共財としての情報を人類全体として有用に活用する手法が求められるのである。

4.4. AIによる情報インテグレーション

さらに問題となるのが，AI（人工知能）の進化である。ビッグデータ解析にAIが不可欠なのはいうまでもないが，AIがシンギュラリティ[28]以降，情報インテグレーション技術の駆使を自発的に行えば，人類には及びもしない情報管理社会が生まれてくる[29]。

DNAデータの集約による発病リスクの予測，気候変動による災害リスクの予測，人身事故発生予測等が可能となりポジティブな未来社会予測が可能となる一

[28] Ray Kurzweil, *The Singularity is Near: When Humans Transcend Biology* (2005)，邦訳『ポスト・ヒューマン誕生 コンピューターが人類の知性を超えるとき』井上健監訳他 NHK出版 2007年。
[29] 伊藤博文「法的特異点について」愛知大学情報メディアセンター紀要『COM』Vol. 26/No. 1第41号13頁（2016年），*available at* http://cals.aichi-u.ac.jp/products/articles/OnJudicialSingularityV1.pdf。

方で，個として埋没する個人情報の範囲（プライバシー・ライン）がAIにより決定されるようになり，全体の利益のために没個性が強く要求される社会になる。

情報処理演算能力の向上，情報インテグレーション技術の向上，情報収集技術の向上と深化（IoT，GPS，スマホの通信データ，SNS上での情報発信，遺伝子情報解析の普及等），AIが自律的に情報インテグレーションを行うようにするのは大きなリスクが伴う。特に，汎用人工知能（AGI: Artificial General Intelligence）のように，自己学習するAI，自ら情報を取りに行くAI，強いAIと呼ばれる段階のAIが情報インテグレーションを管理するとき，もはや人類はAIの完全なる管理下におかれることとなる。

AIが細胞レベルの小さなチップになれば，人はサイボーグ化されたものになり，将にHybrid Humanの出現となる。近未来の人間は，バイタルデータやDNA情報等が逐次AIの持つセンサーにより自動記録・管理されることとなろう。このような時代にプライバシーを論ずる意義を再考する必要があろう。

5. おわりに

ここまで情報インテグレーションについて考察してきたのであるが，残念ながら，指摘してきた問題点への決定的な対処方法が見出せないのが実情である。今後の研究に大いに期待するところである。

現状で考え得る一つの方法としては，情報インテグレーション権（Information Integration Right）を構想していく方法が考え得る。また今後の開発されるテクノロジーを駆使して，情報データに対しブロックチェーン（Block Chain）技術を駆使して情報のトレーサビリティを確保して情報管理することも一案となろう。

いずれにせよ，誰がどうやって認めるのか社会的なコンセンサスが不可欠である。営利追求を前提としたビジネスは匿名化されないビッグデータを欲しがる。しかし市井の人々は自らの情報を安易に提供することには躊躇いがある。この両者のバランスをどう保つかという社会的に議論が必要とされる。この論稿が今後のその議論の一助となれば幸いである。