Vol.2013-DPS-156 No.20
Vol.2013-GN-89 No.20
Vol.2013-EIP-61 No.20
2013/9/13

ビッグデータ社会における「個人データ」保護のあり方の検討 ～ナッジによる規制の提案～

石田 茂[†1]

近年，IT の進展の伴い，ビッグデータビジネスが注目を集めている．企業が収集した個人データの利活用については，多くの可能性が期待されている一方，プライバシーに関する様々な懸念も指摘されている．本稿では，レッシグの規制の 4 要素（法，規範，市場，コード）に対し，新たに「自己防衛」と「ナッジ」を加え，それらの要素の組み合わせによって，「個人データ」を保護する方法を提案する．また個人データ管理における企業の責任についても課題を示す．

Six factors for protection of "personal data" in the big data society

SHIGERU ISHIDA[†1]

Today with the progress of IT, Big data business attracts attention. Indeed, great benefits may be generated by useing the personal data properly. But at the same time, various concerns about the privacy are pointed out. In this article, we propose six factors of protection that added "Self defense" and "NUDGE" to four factors (law, norms, markets, cord) of the regulation which were defined by Lessig. We also refer to the responsibility of the company in the personal data management.

1. はじめに

今日，携帯電話やスマートフォン，IC カード，GPS（全地球測位システム），twitter や facebook などに代表されるインターネット上の SNS サービスを通じて，個人の生活に関する多種多量な情報（ライフログ）が取得・蓄積されている．これらの多種多量のデータを「ビッグデータ」と呼び，事業に役立つ知見を導出するためのデータと位置付け，また，それらを用いて社会・経済の問題解決や業務の付加価値向上を行う事業としての「ビッグデータビジネス」が注目を集めている．

ビッグデータを活用したサービスの例としては，利用者の購買履歴を分析し「おすすめ商品」を提示するものや，利用者の Web サイトの閲覧状況（行動履歴）を分析し，顧客の関心に応じた広告を表示するもの等があげられる．これらのサービスの提供は，事業者にとっては収益向上に寄与し，また利用者にとっては利便性の向上というメリットがある．利用者にとって，利便性向上のメリットがある反面，このようなビッグデータには，個人に関する情報が含まれるため，本人の知らない間にプライバシーが侵害されているのではないかとの懸念が持たれている．

プライバシー侵害に関する懸念の最近の事案として，JR 東日本の Suica データ販売問題がある．JR 東日本は Suica の乗降記録データを匿名化した上で日立製作所に販売していたが，JR 東日本が Suica データの販売の事実や販売したデータの内容を利用者に事前に公表していなかったため，ネット上で大きな話題となり,マスコミでも取り上げられた．最新の報道（7 月 26 日時点）では，JR 東日本は利用者からの要望があれば,日立製作所に販売するデータから当該利用者のデータは除外するとのことである[1].

このような混乱を避けるために，個人情報保護法の理念である「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」に照らし，保護法益と利益考量の両面で，個人に関する情報を含むビッグデータ活用のルールを社会制度として検討する必要がある．

ローレンス・レッシグは，社会制度を設計し運用する場合に,《法》,《規範》,《市場》,《コード／アーキテクチャー》の 4 つの要素があり，その組み合わせで実現されるとした[2]. 本稿では、レッシグの規制の 4 要素（法、規範、市場、コード）に，新たな規制要素として,《自己防衛》と《ナッジ・デザイン》を加え，それらの要素の組み合わせによって，「個人データ」を保護する方法を提案する．

個人データを保護する方法に，唯一絶対のものは存在しない．上記各要素の組み合わせによる解決策を模索すべきである．社会的に保護すべき利益は複雑に絡み合っているため，私的／公的な利益でバランスを取った制度設計が行われるべきである．技術革新のスピードが速く，多様な価値観を持つ人々が複雑に関係する現代社会においては，ハードな定型的な方法より，ソフトな柔軟な方法に期待が高まるものと思われる. 本稿で提案するナッジ･デザインは，柔軟性のある解決策の一つであると考える．

†1 情報セキュリティ大学院大学
Institute of Information Security

Vol.2013-DPS-156 No.20
Vol.2013-GN-89 No.20
Vol.2013-EIP-61 No.20
2013/9/13

2. プライバシー保護の手段としての「個人データ」保護

2.1 プライバシーと個人情報，個人データの相違

「プライバシー」と「個人情報」の両者の違いについては，必ずしも明確に区別されずに議論されることが多く，そのことにより，両者の概念が混同されていると言える．

プライバシーとは，辞書（小学館「大辞泉」）によると，「個人や家庭内の私事・私生活．個人の秘密．また，それが他人から干渉・侵害を受けない権利」とある．

個人情報保護法において，個人情報とは，「生存する個人に関する情報であって，当該情報に含まれる氏名，生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ，それにより特定の個人を識別することができることとなるものを含む）」（2 条 1 項）のことであり，個人データとは，「個人情報データベース等を構成する個人情報」（2 条 4 項）である．ここで「個人情報データベース等」とは，「個人情報を含む情報の集合物であって，特定の個人情報を電子計算機を用いて検索することができるように体系的に構成したもの，およびそれに準じるもの」をいう．

個人情報保護法は，個人情報の適正な取扱と保護について定めた法律であり，「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とする」（1 条）としており，「プライバシーの権利の保護」を目的としてはおらず，法律の条文においても，「プライバシー」という用語は用いられていない．

本稿において，「個人データ」[a]とは，個人情報保護法の定義より広い範囲で，「ライフログを含む個人に関する多種多様なデータ」という意味で使用する．図 1 に，「個人情報」，「個人データ」と「プライバシー」の関係を示す．

2.2 個人データ保護とプライバシー侵害の関係

プライバシーの権利は，米国において 1890 年にウォーレンとブランダイスが著した「プライバシーの権利」にて，「一人にしておいてもらう権利(right to be let alone)」としてのプライバシーの権利が主張されたのを端緒とし，不法行為法上の権利として，また，合衆国憲法上の権利として確立していった[4].

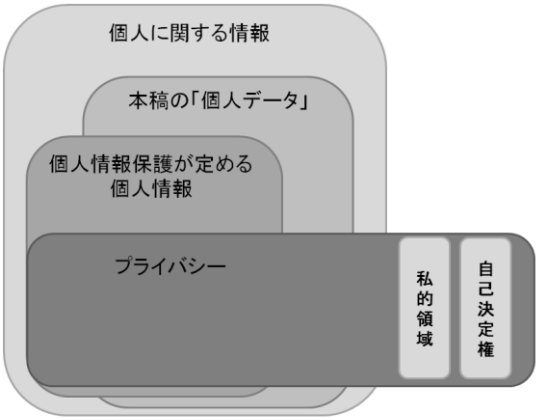

図 1 個人情報，個人データ，プライバシーの関係

日本においては，プライバシーの権利は，憲法の幸福追求権（憲法 13 条）を根拠とする学説が通説となっている[3].

1964 年の「宴のあと事件」[b]によって，プライバシー権は「私生活をみだりに公開されないという法的保障ないし権利」として承認された．本判決は，プライバシーの侵害による不法行為の成立要件として，以下の 3 つの要件をあげている．

①公開された内容が私生活の事実又はそれらしく受けとられるおそれのある事柄であること
②一般人の感受性を基準にして当該私人の立場に立った場合，公開を欲しないであろうと認められること
③一般の人々に未だ知られない事柄であること

本判決を契機として，プライバシー権は「私生活をみだりに公開されないという法的保障ないし権利」として発展していった．

さて，例えば，事業が保管している個人情報が漏洩した場合，単に漏洩が生じたという事実をもって，プライバシーが侵害されたと言えるだろうか．プライバシーが侵害されたか否かは，専ら当該個人の感受性に依存している．それは時（time）と場所　（place）と態様（manner）など状況（context）よって，同一人に対しても変動し得る概念である．プライバシー侵害は，事後的な評価と救済で対応せざるを得ない．

一方個人データ保護は，漏洩によるプライバシー侵害を生じるリスクを低減する手段と位置付けられる．事業者の故意・過失による個人情報の漏洩や不適切な利用を未然に防止するため，事前に必要な対策を実施することが求められる．

プライバシー侵害と個人データ保護は，事後と事前の関係であり，区別して扱う必要がある．本稿では，個人データ保護のための事前の対策に焦点を当てる．

a 経済産業省および総務省では，同様の概念を「パーソナルデータ」と定義している．本稿では，「個人データ」という用語を用いたが，不要な概念の混乱を避けるため，今後は「パーソナルデータ」に改めたい．
経済産業省：IT 融合フォーラム パーソナルデータワーキンググループ報告書(平成 25 年 5 月)
総務省：パーソナルデータの利用・流通に関する研究会報告書(平成 25 年 6 月)

b東京地判昭和 39 年 9 月 28 日判時 385 号 12 頁

Vol.2013-DPS-156 No.20
Vol.2013-GN-89 No.20
Vol.2013-EIP-61 No.20
2013/9/13

3. 個人データ保護のための規制要素

3.1 レッシグの四規制要素

レッシグは，人のふるまいに影響を及ぼすすべてのことを「規制」と定義づけており，規制要素として、「法律(law)」，「規範(norms)」，「市場(markets)」，「コード(code)／アーキテクチャー(architecture)」をあげている[2].

「法律」の規制は，制裁の脅しに裏付けられた命令による規制である.「規範」の規制は，社会やコミュニティの不文律による規制である.「市場」の規制は，価格や企業の評価を通しての規制である.「コード」の規制とは，ハードウェアとソフトウェアがサイバー空間を規制・制御する際の規律による規制である，例えば，パスワードがないとアクセスできないサイトや実名でないと登録できないサイトなどである.

プライバシーについて，レッシグは次のように言及している.「技術の向上により，人々のふるまいの永続的で安上がりな監視が可能となった．個人が適切なコントロール水準の回復のために,「法律」と「技術」をいかにミックスするかを検討しなければならず，また，その水準は私的／公的な利益でバランスを取らなければならない」としている[2].

3.2 個人データ保護のための規制要素

レッシグは前述のとおり 4 つの規制要素を示した．林はこれらが個人データ保護にも応用可能であるとし， 6 つの規制要素に拡張した．6 つの規制要素とは,《法律》,《組織規律》,《市場価値》,《自己防衛》,《ナッジ・デザイン》,《技術》である[5].

以下，林の案を踏襲し，補足的に説明する．ここで，レッシグの《規範》は，個人情報の利用者側と情報の帰属者側に分解されると考えたことより,《組織規律》と《自己防衛》に分け,《コード／アーキテクチャー》は実現手段としての《技術》と，設計思想としての《ナッジ・デザイン》に分けている.

(1) 法律

国家が強制力をもって，人（自然人及び法人）を規制し，違反した場合にはサンクション（制裁）が課せられる．人の行動を規制する法的手段のあり方としては，以下の 3 つの要素がある[6].

①介入のタイミング（行為の前／行為の後）
②介入の形式（阻止／サンクションの賦課）
③私的介入／公的介入（民事訴訟，刑事訴訟・行政行為）

プライバシー侵害は，事後に不法行為法（民法 709 条）に基づき，民事訴訟を経て，損害賠償請求により，被害の救済が行われる．わが国では，懲罰的損害賠償は認められず，介入の形式は，不法行為による損害賠償責任を通じた間接的な「抑止」の効果がある．一方，個人データ保護の場合，個人情報保護法では，事前に，データ提供者の権利利益の侵害を阻止し，事後に公的介入をおこなう構造となっている.

(2) 組織規律

企業は社会から企業倫理としての組織規律が期待される．個人データを大量に保有している企業のなかには，法令遵守の一環として，個人情報保護法を遵守するために個人情報保護の取り組みをおこなうだけなく，「個人データ」に関するより高い水準での保護を達成するため，自主規制として，プライバシーマークなどの第三者認証の取得・維持に取り組むものもある.

(3) 市場価値

競争原理に基づく市場の機能である．経済学者のフリードマンは以下のように述べている.「われわれの世界はけっして完全ではない．そこにはつねに貧弱な商品があり，ニセ医者や詐欺師がいることだろう．しかし概していえば，市場競争がその働きにまかせてもらえれば，今日ますます市場に対して上から押し付けられてきている政府による規制やその他の活動よりも，消費者をはるかによく保護してくれる」としている[7].

つまり，消費者から信頼を得られない企業は，やがては淘汰されるということである．しかし，個人データを提供する側と利用する企業の間には，情報の非対称性が存在するため，粗悪なサービスしか提供されなくなると，その市場は成立しなくなる[c]．よって，企業側にも，個人データ保護に対する自己の取り組みの自主的な公開や第三者認証の取得等による，情報の非対称解消への誘因（インセンディブ）が働く理由がある.

(4) 自己防衛

個人データが帰属する個人の側には,「自己防衛」という責任も期待される． 日本の消費者，特に若年層は，自衛手段による個人情報保護対策の実施率が低く，企業や社会の保護対策に委ねる傾向が強い[8].

ソーシャル・ネットワーキング・サービス（SNS）で，青少年が自分の情報を安易に晒したり，他人の情報を公開し，プライバシー侵害にまで発展するなど問題になっているが,情報リテラシーを育むことが現代の規範とも言える.

(5) ナッジ・デザイン

辞書（研究社 新英和中辞典）によると、ナッジ（nudge)とは「(注意を引くためひじで)〈人を〉そっと突く,〈…するように〉〈人を〉そっと突く［押す］」とある． セイラー

c いわゆる「レモン市場」の原理である．レモンとは，食物のレモンではなく，中古車のことを指している．中古車を売る側は故障個所といった情報を把握しているが，その情報は中古車を買う側には分からない．また，買う側にとっては，中古車を買う前にその品質を見極めることは困難であるため、買う側はなかなか中古車を買わないか，もしくは適切な価格よりも大幅に安くなければ買わなくなる．したがって，売る側にとっては，適正な価格を維持するために，情報の非対称解消への誘因（インセンディブ）がある.

Vol.2013-DPS-156 No.20
Vol.2013-GN-89 No.20
Vol.2013-EIP-61 No.20
2013/9/13

&サンスティーンは,「人々を強制させることなく望ましい行動に誘導するようなシグナル，または仕組みのこと」をナッジ(nudge)と呼んでいる[9]．彼らは，人間は必ずしも，合理的に判断し最適な選択を行ってはおらず，ナッジを適切に組み込むことによって，人々がより良い生活が送れるよう自発的に取り込むことができるとし，人々の選択をナッジにより支援する仕組みを「選択アーキテクチャー」と呼んでいる．そして，良い選択アーキテクチャーをつくる6原則として，以下をあげている．

・インセンティブ（i**N**centives）
・マッピングを理解する（**U**nderstand mapping）
・デフォルト（**D**efaults）
・フィードバックを与える（**G**ive feedback）
・エラーを予期する（**E**xpect error）
・複雑な選択を体系化する（**S**tructure complex choices）

ナッジ・デザインとは，ナッジの考え方を「デザイン（設計）」に取り込む概念であり，後述するプライバシー・バイ・デザインに通じるものである．

(6) **技術**

ここでは個人データ保護に資するための技術の総称である，プライバシー強化技術（Privacy-Enhancing Technologies，以下 PET と記述）が相当する．PET とは，不必要又は違法な処理を防ぐことにより，個人データに関するコントロールを強化するためのツール，あるいは，データ提供者にコントロールを提供することにより，情報システムにおける個人データ保護を強化する情報通信技術のことである．

個人データ保護について，上記のような要素を組み合わせ，私的／公的な利益でバランスを取った制度設計が行われるべきである．社会的に保護すべき利益は複雑に絡み合っているため,どれかを絶対視するのではなく,相対化して見ることが求められる．

4. ナッジ・デザインの実践に向けて

4.1 プライバシー・バイ・デザイン

プライバシー・バイ・デザイン（Privacy by Design，以下 PbD と記述）[10]は，カナダオンタリオ州情報＆プライバシーコミッショナーのアン・カヴォキアンが 1990 年代に提唱したものである．PbD とは，「プライバシー侵害のリスクを低減するために，システムの開発においてプロアクティブ（事前）にプライバシー対策を考慮するというコンセプトであり，企画から保守段階までのシステムライフサイクルで一貫した取り組みを行うこと」である．

PbD は，以下の 7 つの基本原則によって構成される．

①事後ではなく事前に
②プライバシー保護をデフォルト設定とする
③プライバシー対策は設計時に組み込む
④ゼロサムではなくポジティブサム
⑤エンドツーエンドのライフサイクルで実施する
⑥可視化と透明性
⑦ユーザーのプライバシーを尊重する

PbD の実践として，個人データを推定されてもプライバシー侵害につながらないように匿名化などの処理を施すことがあげられる．ナッジ・デザインの例としては，個人データの利活用を想定する際に，サービス提供者に対し，PdD のソリューションを提示し，サービス利用者に対しては，サービス提供者が個人データに対する匿名化処理の組み込みをおこない，プロセスの透明性を確保する仕組みを構築していることをガイドするなどが考えられる．

4.2 防犯環境設計のアナロジーとしてのナッジ・デザイン

ナッジ・デザインの実践を，防犯環境設計のアナロジーとして考察する．

防犯環境設計とは，犯罪が発生する物的な環境や状況に着目した犯罪予防の手法であり，CPTED(Crime Prevention Through Environmental Design)とも呼ばれている[11]．物的な環境を適切に整備・管理し，効果的に利用すれば，犯罪の機会を減らすだけでなく，犯罪不安を軽くし，人や社会の生活の質を向上させることができるという考え方に基づいている．防犯環境施設計には，直接的な手法として,「①被害対象の強化・回避」と「②接近の制御」，間接的な手法として,「③監視性の確保」と「④領域性の強化」があり，これらを組み合わせて行う．

①被害対象の強化

犯罪の被害対象になることを回避するため，犯罪の誘発要因を除去したり，対象物の強化を図ることである．

・出入口や窓の鍵を強化する
・警報装置や防犯カメラなど設置する

②接近の制御

犯罪者が被害対象に近づきにくくすることにより犯罪を未然に防ぐことである．

・庭の周囲を塀で囲う
・上方への足場を少なくする

③監視性の確保

多くの人の目が自然に届く見通しを確保することである．

・外部照明の改善
・街路や窓からの見通しの確保

④領域の強化

共用のエリアに対する住民のコントロールを強めることである．

・不法投棄や放置自転車を撤去したり，掃除や落書きを消すなど，住宅やその周辺の維持管理状態を向上させる

Vol.2013-DPS-156 No.20
Vol.2013-GN-89 No.20
Vol.2013-EIP-61 No.20
2013/9/13

・住民の屋外交流を促して，部外者が侵入しくにくい環境をつくる

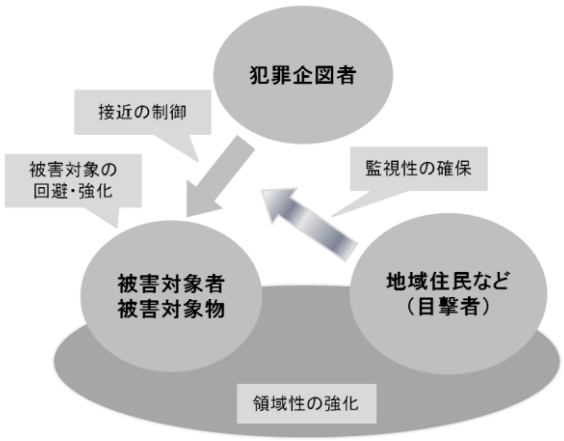

図 2 防犯環境設計の概念

次に，ナッジ・デザインによる個人データ保護に資する環境（つまりシステム）設計を検討する．

ナッジ・デザインは，ナッジの 6 原則を組み合わせ，利用者の選択を支援する仕組みを設計する．

①インセンティブ

サービスを利用することに対するメリットが必要である．例えば，利用者の期待に対する充足度や満足度などがある．なお，サービスを利用するにあたっては，自由な選択が保障されなければならず，オプトイン／オプトアウトが保障されなければならない．

②マッピングを理解する

利便性とリスクはトレードオフの関係にある．サービス利用に伴うリスクを，利用者に正しく認識させる必要がある．また，どの局面でリスクが高いか，その対策についても例示が必要である．例えば，パスワードの設定や管理は利用者の責任に委ねられることなどがあげられる．

③デフォルトを設定する

取得や公開の範囲はデフォルトで設定する．

④フィードバックを与える

利用者の個人データがどのように使われているか，わかるようにする．例えば，アクセス履歴が閲覧できるようにするなどがあげられる．透明性を確保するため，中立的な第三者機関による評価や関与についても検討するべきである．

⑤エラーを予期する

人間は間違いを犯すものである．例えば，重要な処理の前に確認ダイアログを表示したりするなど注意を引くなどあげられる．また，データ管理上のミスの対策として，データ保護のための暗号化や匿名化の処理を検討する．

⑥複雑な選択を体系化する

利用規約やプライバシーステートメントは冗長であり，法的な表現は一般の利用者には,わかりくにいものである．それらを，平易で簡潔な表示したり，ラベル（アイコンやマーク）で表示するなど，利用者に理解しやすいよう工夫することがあげられる．また，利用者が提供するデータは選択可能とし，その際，利用可能なサービス機能や制限について，利用者に理解しやすいよう工夫する必要がある．

5. 法人の責任の課題

5.1 法人の責任

プライバシー侵害などの民事の事案においては，故意や過失で他人の権利を侵害すると，その損害を賠償する責任が生ずる（民法 709 条）が，その主体は行為者すなわち個人である．当該個人を雇っている法人は，事業執行上のことであれば「使用者責任」を負うが（715 条 1 項），「相当の注意を払っていれば免責される（同条但し書き）．

しかし，公害や製造物責任のように事業者の労働者の行為というよりも，企業活動そのものが他人の権利を侵害していると解するのが自然である．

個人データが一度漏洩し，インターネット上で拡散すると，拡散したデータの回収や現状回復は，事実上不可能である．企業の個人データ保護を企業の自主的な取り組みに依存させる以上，責任の主体は法人とするべきではないだろうか．そのため，行為者は罰せられずに法人だけが責任を負う制度の検討が必要である．

5.2 コミットメント責任論

林と鈴木は，コミットメント責任という，情報管理に関する法人の責任に関する新しい考え方を提案している[12].

「コミットメント責任」とは，「事業者が，情報管理の取扱いに関する約束事を消費者に対して表示し，または社会に対して宣言したにもかかわらず，それに違反することによって生じる責任（法的責任を中心としながらも，より広い概念としての責任，免責を含む)」である．

コミットメント責任を組み込んだ制度として，米国のプライバシー保護に関する第三者評価制度である TRUSTe がある．TRUSTe は，事業者がプライバシーステートメントやポリシーをウェブサイト上に表示することで，消費者との間で一定のコミットをするよう制度要請されている．つまり，自己宣言を基調とする制度となっており，消費者に対して表示と異なる欺瞞的な行為をした場合は，FTC（連邦取引委員会）の調査権の発動を招く．民間の第三者認証制度が，法律との補完関係によって一定程度の消費者保護の実効性を確保できる例として参考になる[13].

6. おわりに

本稿では，「個人データ」保護のための，レッシグの規

Vol.2013-DPS-156 No.20
Vol.2013-GN-89 No.20
Vol.2013-EIP-61 No.20
2013/9/13

制の 4 要素（法，規範，市場，コード）に，新たに追加する規制要素の「ナッジ」を中心に解説した．

防犯環境設計は，物的な環境を適切に整備・管理し，効果的に利用すれば，犯罪の機会を減らすだけでなく，犯罪不安を軽くし，人や社会の生活の質を向上させることができるという考え方であるが，ナッジ・デザインも，防犯環境設計のように，個人データ保護に資するシステム設計の思想となりうると考える．

個人データを保護する方法に，唯一絶対のものは存在しない．《法律》,《組織規律》,《市場価値》,《自己防衛》,《ナッジ・デザイン》,《技術》の各要素の組み合わせによる解決策を模索すべきである．

社会的に保護すべき利益は複雑に絡み合っているため，私的／公的な利益でバランスを取った制度設計が行われるべきである．技術革新のスピードが速く，多様な価値観を持つ人々が複雑に関係する現代社会においては，ハードな定型的な方法より，ソフトな柔軟な方法に期待が高まるものと思われる．本稿で提案したナッジ・デザインは，柔軟性のある解決策の一つであると考える．

今後，システム構築の要件定義やユーザー・インターフェース設計の分野で，ナッジ・デザインの実践を調査する予定である．

参考文献

1) JR 東日本が Suica データの外部提供について説明､オプトアウト受付も開始
http://itpro.nikkeibp.co.jp/article/NEWS/20130726/494266/
2) ローレンス・レッシグ，山形浩生（訳）: CODE VERSION 2.0, 翔泳社(2007).
http://office.microsoft.com/ja-jp/word-help/CL010072933.aspx
3) 芦部信喜，高橋和之：憲法 第五版，岩波書店(2011).
4) 石井夏生利：個人情報保護の理念と現代的課題 プライバシー権の歴史と国際的視点，勁草書房(2008).
5) 林紘一郎：多様な利益の比較考量を，日本経済新聞経済教室(2013 年 7 月 19 日).
6) スティーブン・シャベル : 田中亘，飯田高（訳）: 法と経済学, 日本経済新聞社(2010).
7) ミルトン・フリードマン，ローズ・フリードマン，西山千明（訳）: 選択の自由―自由への挑戦，日本経済新聞社(2012).
8) 小林慎太郎，八代拓，伊藤智久，奥見紗和子：ビックデータ社会におけるプライバシー「個人情報」から「プライバシー」の保護へ, 知的資産創造, 2012 年 9 月号, pp.36-55,野村総合研究所(2012).
9) リチャード･セイラー, キャス･サスティーン, 遠藤真美（訳）: 実践行動経済学－健康, 富, 幸福への聡明な選択, 日経 BP 社(2009).
10) 高坂定, 瀬戸洋一 : エンジニアのためのセキュリティ入門 プライバシー･バイ･デザイン, 月刊自動認識 2011 年 10 月号, pp.57-64, 日本工業出版社(2011).
11) 子ども安全まちづくりパートナーズ / 防犯環境設計 (CPTED)
http://kodomo-anzen.org/manual/p051/tishiki-16/
12) 林紘一郎・鈴木正朝：情報漏洩リスクと責任－個人情報を例としてー，法社会学，第 69 号(2008).
13) 林紘一郎：第 7 章 法学的アプローチ，松浦幹太（編），セキュリティマネジメント学－理論と事例－，共立出版(2011)