# 情報社会におけるプライバシーと倫理

## Privacy & Ethics of Information Society

長谷川　欽一
PEK 長谷川技術士事務所

Kinichi HASEGAWA
PEK Hasegawa Professional Engineer Office

【Key words】
1. ユビキタス・コンピューティング（Ubiquitous Computing）
2. メディアリテラシー（Media Literacy）
3. ソーシャルネットワーキングサービス（SNS：Social Networking Service）
4. サイバー攻撃（サイバーテロ）（Cyber-Terrorism）
5. プライバシー権（Privacy Rights）

## 【概要】

コンピュータとネットワークというテクノロジーの登場により，わたしたちの生活は「情報」なるものと密接に関わりを持ち始めています．そして，そこに生じる問題は，コンピュータとネットワークの「使い方」を越えて，そうしたテクノロジーとともに生きる私たちの「生き方」や「社会のあり方」にまで及んでいます．現代に生きる私たちは，そのような問題について考察し理解を深めながらあるべき姿を模索していく必要があります．

## 1. はじめに

２０年くらい前の学生の皆さんが生まれたころにインターネットがパソコンと並行して一般にも急速に普及しました．それまではインターネットも一部の大学の研究対象にすぎませんでした．

「１９９２年にインターネットが日本でも商用化され，１９９５年にはマイクロソフトがパソコン用ＯＳの「ウィンドウズ９５」が発売され，インターネットも一般に爆発的に普及しました．１９９９年にＹ２Ｋと呼ばれた２０００年問題への対応が世界的に問題になりました．ＳＮＳの２ちゃんねるもこの時期に誕生しました．２０００年に日本で不正アクセス禁止法が施行され，施行から約１ヵ月後に，他人のＩＤとパスワードを勝手に使用してインターネットに接続したとして岐阜県の男性が逮捕され，この法律による摘発の第一号となりました」[1]．

２００１年にはファイル交換ソフト「Win　MX」を使って著作権の中でも公衆送信権を侵害したとして京都の２人が逮捕されました．２００３年に日本で個人情報保護法が成立し（施行は２００５年４月），２０１５年５月に改正されました（施行は２年以内）．２００４年にファイル交換（ＰtoＰ：ピア・ツー・ピア）ソフト「ウィニー」の作者である東京大学特任助手が著作権法違反の幇助として逮捕されました．一旦有罪判決を受けましたが２０１２年１２月に最終的に無罪となりましたが，ソフト使用者の責任を問われることになり多くの課題をのこしました．また人間の経験や技能をビッグデータとクラウドコンピューティングを使ってＡＩ（人工知能）的に活用しようという試みが多くなされるようになってきています．それに伴って，例えばGoogleの検索で個人名を入力すると個人情報が検索された結果，事実とは異なる悪意のある結果が導き出される例もあり，企業人の場合には退職に追い込まれることもあり再就職困難な状況も生まれています．

このようにインターネットの発達と普及が，限りない倫理問題を生み出しています．そして，そこに生じた問題は，コンピュータとネットワークの「使い方」を越えて，そうしたテクノロジーとともに生きる私たちの「生き方」や「社会のあり方」にまで及んできました．現代に生きる私たちは，そのような問題について考察し，理解を深める必要があります．

## 2.　ユビキタス・コンピューティング

コンピュータとネットワークというテクノロジーの登場により，わたしたちの生活は「情報」なるものと密接に関わりを持ち始めるようになりました.

最近急激に普及したソーシャルネットワーキングサービス（ＳＮＳ）により情報活用による生活の変化が急激に起こっています．私たちは「目に見えない」，また「区別がつかない」ほど多くの情報機器が日常に織り込まれた情報化社会で生活しています.

このように生活の中にコンピュータやネットワークが組み込まれ，意識することなく活用している環境のことはユビキタス・コンピューティングとかユビキタス社会とか言われています．ユビキタスとは古いラテン語「どこにでもある」の意味でユビキタス環境とは「いつでも」「どこでも」「なんでも」とか「誰とでも」「何とでも」接続できる環境のことです[2)3)].

ネットワーク社会では携帯電話・スマートフォン・コンピュータ・テレビ・家電・カーナビゲーションなどのネットワークが新たなコミュニケーションの場となりましたＷｅｂサービスとはＷｅｂサーバーとインターネットによりページのリクエスト, ページ情報の送信, ページの組み立てではテキスト，画像，音楽などです.

検索エンジン（Search Engine）はポータルサイト（Portal Site）とよばれインターネットへの入り口のことです.

検索エンジンはカテゴリー別に分類して検索すると，狭義ではディレクトリ型と広義では全文検索型があります．データベースに蓄えたＷｅｂサイト全文の中からキーワードによって検索します.

このようなビッグデータとクラウド（雲）コンピューティングを使ってＡＩ（人工知能）的に検索エンジンとして活用しようという試みがなされるようになってきました.

検索エンジンへの情報登録は申請に応じて担当者により手作業で行なう場合や，ロボットと呼ばれるプログラムを使ってＷｅｂページの内容やアドレスを収集するロボット型があります[2)].

検索エンジンの運営費は企業の広報手段企業広告の掲載料で賄われているので一般のユーザーは無料で利用できます.

## 3. メディアリテラシー

メディアリテラシーとは，信憑性が高く，信頼性のある「情報」を探し出す力や情報が流通するメディアつまりいろいろな媒体を使いこなす能力のことです．メディアの特性や利用方法を理解し，適切な手段で自分の考えを他者に伝達し，あるいは，メディアを流れる情報を取捨選択して活用する能力のことをいいます．インターネットでは善悪の判断と情報の信憑性の判断はメディアリテラシーが必要です．

つまり，メディアリテラシーとはメディアリテラシー ＝「メディア」＋「リテラシー（情報や知識の活用能力）」のことでメディアとは新聞，雑誌，テレビ，ラジオ，インターネットなどです．

メディアリテラシーを身につけるとは，①Ｗｅｂページの閲覧だけでは身につかない,②友人間だけの電子メールのみでも身につかない,③情報の信憑性を誰かに投げかけ真意を得ること,などが必要です．

メディアリテラシーに関する問題は，①他人の著作物を公開すると訴訟問題になり，②キャラクタが似ていると非難の対象になり,③誹謗中傷も批判の対象になり,④個人情報を掲載するといたずらされる可能性があります．

つまりメディアリテラシーとは，①情報媒体を正しく使いこなす能力,②自ら信憑性を確かめ，情報を選ぶ能力,③ルールは万全でないのでユーザー自身が身につけるべき能力，などとされています．

メディアリテラシーの能力としての情報発信の種類は，Ｗｅｂブログ，個人のＷｅｂページ，学級新聞，電子メール，チャット，インスタント・メッセンジャなどがあります．つまり他人に同感や批判を繰り返すことで，メディアリテラシーが身につけられます[1)2)]．

従来は，電話や手紙などのパーソナル・コミュニケーションメディア，新聞やテレビ・ラジオをはじめとするマスメディアといった伝統的なメディアの利用方法を知っていれば事足りていました．しかし，現在では，急激な技術の進歩によりインターネットや携帯電話などの新しい形態のメディアが台頭しており，こうした新しいメディアの利用にまつわるトラブルや混乱も頻発するようになっています．このため，各メディアの本質を理解し，適切に利用する能力であるメディアリテラシーが重要になってきました．

## 4.　ネットワーク社会のルールとマナー

ネットワーク社会のルールとマナーは，マイナスの要素とプラスの要素が共存する中で多くの管理者の善意によって維持，更新されており，人に迷惑や不安がらせるような行為を行わないことや，何より相手に対する思いやりや，危険なところや怪しいところには行かないことが重要です．ネットワーク社会ではＳＮＳなど知人とコミュニケーションを深めたり情報を収集したりするのに役立ちますが，機能やルールを理解しないまま使っていると，望まないトラブルが生じる場合があります．

ＳＮＳを含め，ネットでの書き込みは，常に多くの人の目に触れる可能性があることを認識し，Twitter の場合は，特定の相手に一般公開したくない情報を伝えたいときには「ダイレクトメッセージ（ＤＭ）」機能を使たり，Twitter ではなく，メールなど別の連絡手段を使った方が無難です．また，ＳＮＳには意見の異なるユーザーが数多くおり，自分の意見が一般的であると決めつけて書き込むと，気軽な雑談が不毛な議論に発展し“炎上”する可能性がありますので,きわどい内輪話は禁物です．

メッセージやコメントでやり取りしただけの相手とも“友達関係”を結ぶケースが多くあります．そのため，特定の話題で賛同し合えた友達が，他の話題では正反対だったということもありえます．自分の常識を主張し過ぎないように気をつけて気軽な雑談を“炎上”させない配慮が必要です．投稿者が匿名で使っていても，過去のツイートや関連するＳＮＳの情報などから実名やプロフィールが突き止められ，ネット上で“さらしもの”にされたりすることもあります．最近の事例で多いのは，飲食店や販売店の従業員が有名人の来店情報を書き込んだことで“炎上”するパターンで顧客のプライバシーを侵害したとして，勤務先が自社サイトに謝罪文を掲載する事態に発展しています．

つまり、情報倫理における「ルールとマナー」とは,①人に迷惑をかけないか,名誉毀損などにあたる書き込みをしていないか,②自分が犯罪に巻き込まれないか,詐欺や個人情報流出などの危険はないか,③違法行為に当たらないか,違法サイトを見ていないか,④ウイルス対策をしているか,コンピュータやシステムが危険にさらされないか，などです[1)2)]．

## 5. 情報倫理におけるセキュリティ対策

セキュリティ対策では電子メールを利用した犯罪を防ぐ必要があり，コンピュータ・携帯電話などで電子メールが高い利用率がある中で，スパムメール，フィッシング，メールの盗み見やいじめなどが増加しています．

スパムメールでは，広告メールなどでアドレスを生成し無差別に送信されます．特定電子メール法・改訂特定商取引法はスパム配信の取締を行い，未承諾広告の明示義務がある中でフィルタリング機能の活用，記号も含めて長めのアドレス設定（８桁以上）などで自己防衛を行います．また，カメラ付き携帯による被害や，静止画や動画の撮影機能が付いた携帯電話の撮影機能を悪用し，交際相手に恥ずかしい写真を撮られ掲示板にアップロードされ中傷される被害は一瞬で広がりますので相手の気持ちを考え，撮影機能を悪用しないことが大事です [4]．

スパムメールの一種でクロスサイト・スクリプティングと呼ばれる場合はアクセスするとページ内容が書き換えられ別サイトへ誘導されてしまうことを言います．また，ブラウザーでスクリプト（プログラム）の実行を許可すると危険がともないますので，広告等の閲覧で付与された Cookie の情報を持ち出されないように削除しておくことをお勧めします．

不正な情報収集の例で，フィッシングとは，偽装メールを餌としてアンケートフォームなどで個人情報を釣り上げます．クリックすると本サイトではなく偽装サイトへ誘導されてしまいます．防止対策としては画面だけでは見分けがつかないので，本サイトと偽装サイトのＵＲＬ（ＰＣの上部に表示されている）を比較してチェックすると見破ることができます．

メールの盗み見を防ぐためには，まずメールの暗号化が有効です．メールサーバーは平文で登録しておきます．管理者は覗くことができますが刑法の信書開封に抵触するので管理者のモラルで守るしかありません．他人に覗かれる可能性があり，勝手にメールを削除される可能性があるので，席を離れるときはログアウトします．法的には，他人のユーザーＩＤやパスワードを勝手に使用したり,教えてはいけないという不正アクセス禁止法 [2]違反，有線電子通信法違反，民法違反，刑法違反，個人情報保護法に抵触の可能性があります．Ｗｅｂページ，電子掲示板，チャット，電子メールなどのインター

ネット上での名誉毀損や侮辱行為に対しては主に製作者や管理者への抗議や相手にしないなどの対応が求められ，プロバイダやひどい場合は警察への通告が必要です．

ネットオークションでのノークレーム・ノーリターンでの取引は法的には返品可能です．偽ブランド品の売買はオークション開設者と警察への届出をします．入金金額の錯誤は，入札者へ謝るなどします．場合によっては損害賠償の対象となります．入金しても商品が送られてこない場合もあります．睡眠薬や劇物の売買は薬事法，民法，刑事法により罰せられます．

ウイルスを仕掛ける行為は不正アクセス禁止法違反で民法 706 条の不法行為となります．プログラムの改ざんを含むウイルスは刑法 161 条の電磁的記録不正作出及び共有罪，刑法 234 条の電子計算機損壊等業務妨害罪，民法 709 条の不法行為，不正アクセス禁止法に抵触します．ウイルスの製造や保持に関し，製造だけでは問われませんが，ネットワークを通じて配布または配布できる状態にある場合は，刑事罰の対象になります．ウイルスの保持は製造同様に，保持しているだけでは違法ではありませんがネットワークを通じて配布した場合，社会的責任が生じます．

個人情報の流出のケースはアンケートや懸賞などで漏洩したり，占いサイトから漏洩したり，スパイウェアから盗まれたり，学校などの団体からの流出や，インターネットの経路途中で覗き見されるなどたくさんのケースが考えられます．不正アクセスされた場合下記の対策を行うことで支援が得られるのでセキュリティ対策をわかる範囲で行い，分析可能なログを残し，システム設計に関わる資料を保存しておきます．

セキュリティ対策を採る場合，アクセス制限が無い場合，妨害されたことにならず，したがって不正アクセスに当たらないのでログをできるだけ残すことが重要です．システムのログや掲示板，チャットなどのログも重要になります．セキュリティ対策を検討し，支援を受ける意思が重要で，知識を学ぶための費用と時間を費やします．不正アクセスの被害にあった場合，サーバーをネットワークから切り離し，現状のバックアップを取り，警察や公安委員会に報告し，復旧作業に取り掛かり，ログの解析を行い再発防止策の策定などが必要となります．

## 6. ソーシャルネットワーキングサービス（SNS）

ネット上には多数のＳＮＳが存在します．「Facebook（フェイスブック）」「mixi（ミクシィ）」「Google＋（グーグルプラス）」「Twitter（ツイッター）」「LINE（ライン）」などそれぞれに特徴があります．無料のミニゲームで知られる「GREE（グリー）」,DeNA の「Mobage（モバゲー）」もＳＮＳの一種です．

「自分の行動や写真が第三者に筒抜けになっている」「不審な人から友達申請が頻繁にくる」「もう，この人の投稿は見たくない」などＳＮＳが普及するのに伴い，それに関連するトラブルも急増しています．

「公開設定」では「いいね！」や「タグ付け」で筒抜けになってしまいます．各サービス毎に設定できる，「近況」「ツイート」「投稿」で記入した内容の公開範囲では，Twitter はブログに近く，公開が原則ですが，逆に LINE は知人だけで使うことを前提にしているので Twitter に比べ公開範囲が狭いのが特徴です．Twitter は通常，誰でもフォローでき自分をフォローする人（フォロワー）を制限したいとなると，設定画面で「ツイートを非公開にする」をチェックするしかありません．これで，他のユーザーがフォローしようとしても，自分が承認しない限り，つながることはありません．誰でもフォローできるのが原則の Twitter も「ツイートを非公開にする」という設定（鍵付きアカウント）にすれば，こちらが承認した人にしかフォローされなくなります．

Facebook の初期設定では，誰からも友達申請が届きますが，これを「友達の友達」に限定すれば，赤の他人が申請してくる可能性は少なくなります．公開範囲設定後に友達が自分をタグ付け（友達の名前を表示する）すると，携帯電話などのアドレス帳が取り込まれて友達候補が推測され「お知らせ」に通知が来ます．別の画面で「隠す」ボタンを押せば，タイムラインには掲載されなくなります．Facebook では，自分と関連がありそうな人を「知り合いかも？」として表示します．共通の友達がいたり，出身校，勤務先，年齢などが近かったりする人などが，友達の候補になります．ユーザーの登録情報などをもとに友達の候補を表示するので，自分に全く関係ない人が表示されることもあります．携帯電話や Gmail などの「アドレス帳」も友達候補の表示に使われているため，サーバーに各自の連絡先がアップロードされます．

公開設定の投稿は「いいね！」の連鎖で広がります．Facebook にアップロードされているアドレス帳データは，Web 上で確認できます．ここに面識のない人が登録されていると，むやみに自分が紹介されてしまうことにつながるので，削除します．知らない人からの友達申請（リクエスト）が煩わしいなら，リクエストを出せる人を「友達の友達」に制限すれば個人情報の取得目的で友達になろうとする悪質ユーザーからの申請もかなり防げます．

LINE は知人だけで使うことを前提にしているので公開範囲は狭く，友達と指定した人のみが公開範囲となります．利用開始時にスマートフォン内のアドレス帳をアップロードでき，アドレス帳に登録があれば，自動的に「友だち」に登録する「友だち自動追加」機能もあります．友達にする相手を自分で選びたいときは，この機能をオフにしておきます．LINE には，アドレス帳をサーバーにアップロードして知り合いを見つけた後に，「友だち」に自動追加する機能があるので，選んだ人だけを追加したいなら，こうした機能はオフにしておきます．

ＳＮＳにはさまざまな利用者がいますので「友達」に登録した相手でも，自分の好みに合わないなどで，投稿を目にしたくない場合があります．ＳＮＳには，友達登録の解除や，迷惑ユーザーとの接触を断つ「ブロック」の機能があります．これらの機能を使っても，いずれは相手に分かります．ＳＮＳでは，「苦手だが，仕方なく友達になってしまった」というケースは珍しくありませんが，迷惑ユーザーを防ぐ「ブロック」機能を拙速に使うのは考えものです．不用意に相手の気分を害さないためにも，悪質なユーザー以外は「非表示」など必要最低限の措置にとどめておいたほうが無難です．

Facebook では，「プライバシーショートカット」を選び，相手のメールアドレスを指定して「ブロックする」ボタンを押すと，そのユーザーとの接触を一切断つことができます．本当に悪意を感じる相手でなければ，「非表示」や「制限リスト」など，相手に知られにくい機能を使うのがお勧めです[4]．

スマートフォンのメッセージアプリの使用のＴＯＰ３を記載した記事では，日本では LINE が首位となっていますが，各国の首位は，米国が Facebook Messenger，中国は WeChat，インドネシア・ブラジル，南アフリカは Facebook が買収した世界 No1 アプリの WhatsApp(ワッツアップ)となっています[5]．

## 7. サイバー攻撃

サイバー攻撃（サイバーテロ）の例としては,２０１５年にＴ大学のサーバーにおいて，送り元のＩＰアドレス（ネット上の住所）が海外の米国，中国，インドの３カ国から相次いで不正なアクセスを受け，アメリカの企業へのサイバー攻撃の一種である「ＤＤｏＳ（ディードス）攻撃」の中継点として悪用されていました．身元を隠すため，複数のサーバーを悪用して乗っ取り，攻撃を肩代わりさせ，情報流出の拠点にするケースです．

サーバーは外部から誰でもアクセスできる状態だったほか，セキュリティ対策も最新型に更新されていませんでした．大学のコンピューターシステムは学術研究の目的で，世界のネットと直結するＩＰアドレスを優先的に割り当てられています．その分サイバー攻撃の標的にされやすく，厳重なセキュリティ体制が求められます．Ｔ大学のサーバーのパスワード（123456：世界中で一番多いＰＷ）は初期設定の単純なままでした[6]．

また日本年金機構も２０１５年６月１日，職員の端末がサイバー攻撃を受け個人情報約１２５万件が外部に流出したと発表しました．いずれも加入者の氏名と基礎年金番号が含まれ，うち約５万２０００件には住所や生年月日も含まれていました． 同機構によると，電子メールの添付ファイルを開封したことで端末がウイルスに感染し，不正アクセスを受けたということです．同機構は警察に通報し，捜査を依頼しました．

情報流出は５月２８日に判明しましたということでしたが実際はかなり前から流失していた模様です．基幹システムである社会保険オンラインシステムへの不正アクセスは今のところ確認されていないようですが，さらに調査中とのことです．

個人情報を管理するサーバーに接続するパソコンを，メール処理に使うなど外部ネットワークにつなげていることは，ほかの官公庁では考えられない状況でした（後に監督官庁である厚生労働省も同様のサイバー攻撃を受けていたことが分かりました）．

また対応の遅さも目に付き，最初に感染が確認されたのは２０１５年５月８日であるにもかかわらず，機構内の全パソコンを外部から遮断したのは２

９日になってからでした．感染が拡大していた２０日間，外部ネットワークとつながっていた状況をずっと放置していたことになります．

公表前にもかかわらず，職員と思われる複数の人物がＳＮＳの「２ちゃんねる」に「ウイルス感染しました」と報告していました．「あれほど，差出人不明メールは開封するな,と警告があったのに」「全職員はパスワードを強制的に変更させられました」「月曜日には,ウイルス感染を公表するのかな？」といった，職員にしか分からない内容が５月３１日までに何度も書き込まれていました．

日本年金機構の個人情報流出問題で，８日にはファイル共有サーバーにデータを移すために渡された年金情報の入ったＤＶＤを，職員が作業後も手元に保管できる運用になっていることが分かりました．外部への持ち出しも可能な状態で，セキュリティ意識の甘さが問われています．

基幹システムに保存されている年金情報はファイル共有サーバーにデータを移して利用します．これらはネットワークでつながっていないため，ＤＶＤを介してデータを移しています．ＤＶＤは職員から申請を受け，システム部門が用意しパスワードとともに渡しますが，データを移し終えた後もすぐに回収されず，職員は手元に置くことができＤＶＤをパソコンに読み込ませた後，そのまま手元で保管するケースもあると指摘されました[7]．

インターネットバンキングの利用者を狙った，駆除しても消えない“ゾンビ型”の新種ウイルスによるサイバー攻撃も国内で相次いでいます．利用者は暗証番号などを盗まれたことに気付かないまま現金を引き落とされる恐れがあります．新種ウイルスは，金融機関のサイトにそっくりな偽画面を表示し，暗証番号などを入力させて盗み取ります．同時にＰＣの通信設定自体も書き換えてしまうため，対策ソフトで「駆除」となった後も誤作動させ続ける“ゾンビ型”とされています．

インターネットバンキングとはネットを通じた金融機関のサービスのことで，利用者は銀行窓口や現金自動預払機（ＡＴＭ）に行かずに自宅のパソコンやスマートフォン（高機能携帯電話）で振り込みなどができます．通信環境の整備とともに普及し，日本の銀行利用者の６割以上が使っているとされています．

## 8. 情報格差（デジタルデバイド）問題

米マイクロソフト（ＭＳ）のウェブブラウザーとよばれるインターネット閲覧ソフト「インターネット・エクスプローラー（ＩＥ）」に欠陥が見つかった２０１４年４月末，ネットではＩＴ知識に乏しい人々の混乱ぶりが相次いで報告されました．職場のアナログな上司などを揶揄する声が目立つ中で，一連の騒ぎは根深い「情報格差（デジタルデバイド）」の現状も浮き彫りにしたようでした．

「職場で『とりあえずインターネットの利用を控えるように』という指示が出た」，「なぜか『ヤフーは危ないから使わないほうがいい』という話になり，みんながＩＥでグーグル検索するようになっている」．

ＩＥに深刻な脆弱（ぜいじゃく）性が見つかり，米国土安全保障省が注意喚起したとの報道が広まった２０１４年４月末にツイッター上には，対応に追われる職場での混乱に戸惑う投稿が相次ぎました．中にはＩＥを含むネット閲覧ソフト（ウェブブラウザー）と，ヤフーなどの検索エンジンとを混同した事例も報告され，「助言しようと思ったけど，そもそも『ブラウザー』という言葉が通じない」といった“悲鳴”もありました．

ブラウザーの知識を「基本中の基本」と見なしていた多くのネットユーザーにとって，相次ぐ混乱報告は「初心者」との知識ギャップを改めて突きつけるものでした．ブラウザーには問題となったＩＥのほかにも米グーグルの「クローム（Chrome）」や米モジラの「ファイアフォックス（Mozilla Firefox）」などの種類があります．ただ，ＩＥはウィンドウズの標準ブラウザーという地位もあり，多くの企業や団体がＩＥを前提としたシステムを採用しておりこうした環境も混乱を後押ししました．

家庭電器店で顧客が「インターネットください」と注文したという逸話は今も笑い話として語り継がれています．

また２０１４年４月には，テレビ朝日系ニュースのＦキャスターが，ＭＳのプレゼンテーションソフト「パワーポイント」について「知らない」と発言したことが大きな話題になり，「無知すぎる」と批判が集まったりもしました．

## 9.　プライバシーと個人情報保護

プライバシーの定義はこのところ大きく揺れています.

従来の古典的プライバシー権では「のぞき見されない権利」「干渉されず,放置される権利」つまり“right to be let　alone”（放っておかれる権利）というのが一般的な理解でした.

最近では欧州委員会では“right to be forgotten”（忘れられる権利）を提唱しています.

個人情報を取り扱う事業者の個人情報の扱いに関する義務（収集，保管，開示・訂正についての義務，手順）と管理責任，情報収集や利用範囲などのガイドラインで，企業や団体における個人情報の取り扱いを決めた第３者への個人情報提供を禁止した法律としては「個人情報の保護に関する法律（俗称：個人情報保護法)」があります．学校は文部科学省が別途ガイドラインを作成し，病院や役所などもある程度例外処置が認められています.

内容は，①（個人情報の収集時の義務）個人情報を収集する場合，利用目的や範囲を明示し，正当な手段で取得する．②（正確性・安全性の確保）利用目的を特定し，本人に通知または公表する．情報は適正な手段で取得する．本人の許可なく目的の範囲を超えて利用することはできない．③（個人情報の開示や訂正義務）保有している個人情報を，「正確」かつ「最新」に保つことと，安全性確保のためのセキュリティ対策を講じる．利用目的の達成に必要な範囲内において，個人データを正確かつ最新の内容に保つ．安全管理措置，従業者と委託先の監督をする．④保有個人データは本人の知り得る状態に置き，開示・訂正・追加・削除・利用停止の請求に応じる,などです.

政府は政府の目玉政策でもある成長戦略（高度ＩＴ総合戦略）の重要な柱に，ビッグデータの利活用による新事業・新サービス創出を促進することがあると発表しています．ビックデータの中でも，特に利用価値が高いと期待されている個人の行動，状態等に関するデータであるパーソナルデータが注目されています．パーソナルデータの利活用として，政府のＩＴ総合戦略本部内に，２０１３年９月にパーソナルデータに関する検討会がスタートし，２０１４年６月の「パーソナルデータに利活用に関する制度改正大綱」にまとめられ，パブリックコメントの募集となりました．２０１４年１２月には

「個人情報保護法改正案の骨子」にはパーソナルデータが様々な場面において履歴として蓄積され，それが場合によってはプライバシー権に大きな影響を及ぼすことが指摘されています．それを受けて２０１５年５月の通常国会で「個人情報保護法」の改正案が通過しました．

個人情報の中には個人データが，個人データの中に保有個人データが含まれます．基本的な事項として氏名，住所，性別，生年月日など（基本４情報），国籍および家庭生活などでは親族関係，婚姻歴，家庭状況，居住状況など，社会生活などでは，職業・職歴，学業・学歴，資格，賞罰，成績・評価など，経済活動などでは資産・収入，借金・預金などの信用情報，納税額などがあります．原則非公開で事業者は思想，信条，宗教，人種，本籍地，病歴，犯罪歴などの社会的差別の原因になる事項,勤労者の団結権など団体行動に関する事項,デモへの参加など政治的権利の行使に関する事項,保健医療・家庭生活などに関する事項など収集制限されます[8]．

個人情報を守るためには，無駄な情報は流さない，大切な情報には暗号化をかける，むやみにアンケートや占いサイトに個人情報を入力しない，懸賞サイトに登録しない，出会い系サイトの利用を避ける，ウイルス対策ソフトを導入するなどが必要となります．

ノートパソコンやメディアの紛失・盗難，ファイル共有ソフトの暴露ウイルス感染など個人情報の流出事件が多発しています．自分自身の個人情報が流出被害に遭わないようにするための注意事項は，不審な電子メールや携帯電話のワン切りなどには一切応じない，共用パソコンで個人情報を入力しない，個人情報をＷｅｂページに掲載しない，ＵＳＢメモリやＣＤ・ＤＶＤなどのリムーバブルメディアの置き忘れや盗難に注意するなど必要です．

ある日突然「犯罪者」の扱いを受け，思いがけない退職勧奨を受け，仕事まで失うことになった例はグーグルのインターネット検索サービスを舞台にした実際の出来事で，東京地裁は３月，被害を受けたという男性の訴えを認め，グーグルに検索内容の削除を命じましたが，同社は今のところ応じていません．Ａさんはこのような犯罪について「身に覚えがない」としています．Ａさんはそうした中傷サイトに行き着く経路として,「グーグル・サジェスト」と呼ぶ検索の機能が関係していることを突き止めました.「削除してほしい」．Ａさんはサービスの提供元であるグーグルに要求しましたが，応じてもらえ

ませんでした．法廷で決着をつけるしかないと決心し，２０１１年１０月，グーグルの米国本社を相手取り，表示差し止めを求める仮処分を東京地裁に申し立てました．

また，「彼氏のスマートフォンにインストールしておけば，彼氏の現在のＧＰＳ位置情報を常にチェックすることが可能」というサービス があり，「パートナーが浮気していないか，スマートフォンの利用履歴を，相手に知られずこっそり監視しましょう」というものです．端末利用者である相手に無断でインストールし，データを収集するという部分が，不正指令電磁的記録供用罪に抵触する可能性が，また無断で対象の移動状況をトレースするつまり追尾することが，民法の不法行為として認定される可能性があります．

プライバシーという問題は，非常に分かりにくい問題です．最近の市場の膨張で生じるプライバシーに関する歪みは，大抵の場合は脆弱な部分にしわ寄せが向かい，それがプライバシーでした．

そもそもプライバシーという概念自体，日本国内では，法的に十分定められていない状態です．少なくとも法令の中で「プライバシー」という文言はどこにも出てきませんし，それを事実上扱っているとされる民法第 709 条（不法行為）も，民事訴訟の判例を積み重ねているに過ぎません．それ以外は，いきなり憲法第 13 条（個人の尊重，幸福追求権，公共の福祉）に至りますが，そもそも憲法論自体に諸説がある以上，定めようがありません．

個人情報保護法は，事業者による個人情報の扱い方を定めただけです．そして当初より，難解なプライバシーの議論に巻き込まれないよう，制度設計されてきました．その結果，保護される対象は「氏名に直接紐付く情報」にほぼ絞り込まれ，またその法解釈は産業分野ごとに異なる，という運用がなされています．従って，氏名と便宜上切り離されていればそのデータは個人情報（保護法の対象）でないと主張する事業者も存在します．また各省庁が制定した同法のガイドラインは，およそ５０種類近くと，おびただしい数に上り，雑然とした状況といえます．

自分の手元にあるスマートフォンは，自分だけが支えているわけではなく端末を作る人，回線を提供する人，サービスを提供する人などさまざまなステイクホルダー（利害関係者）がいます [9]．

## 10. プライバシー権

プライバシー権とは，古くは，私生活上の秘密と名誉を第三者に侵害されない権利をいいます．いわゆる「ひとりで放っておいてもらう権利（right to be let　alone）」と考えられていたものです．日本の憲法にはプライバシーの保護を国民の権利として明文化はしていません．その権利の保護は，憲法第 13 条に基づく．その条文は，「すべて国民は，個人として尊重されています．生命，自由及び幸福追求に対する国民の権利については，公共の福祉に反しない限り，立法その他の国政の上で，最大の尊重を必要とする」とあります．プライバシー権とは，この憲法第 13 条の幸福追求の権利をひろく解釈したことによるものとされています．

なお，プライバシーの侵害は被害者からの訴えがなければ成立しません．「三島由紀夫「宴のあと」事件・1961 年 3 月に元外務大臣の有田八郎氏（原告）が,三島由紀夫の小説「宴のあと」の登場人物は，原告と彼の元妻をモデルにしており，原告のプライバシーを侵害しているとして，三島と出版元の新潮社に対して，損害賠償と謝罪文の新聞掲載を求めて提訴した．・1964 年 9 月，東京地方裁判所はプライバシーの侵害を認め，三島側に損害賠償の支払いを命じた．三島側は控訴したが，原告が 1965 年 3 月に死去したため，1966 年 11 月に有田の遺族と三島・新潮社の間で和解が成立した．・東京地方裁判所は一部認容，一部棄却という判決を下した．争点は次の３つである．

（1）プライバシー権が認められるか

個人の尊厳という思想は,相互の人格が尊重され,不当な干渉から自我が保障されることによってはじめて確実なものとなる.そのためには正当な理由がなく他人の私事を公開することが許されてはならない.

（2）プライバシー権侵害の成立基準

プライバシー権侵害の要件は次の 4 点である.①私生活上の事実，またはそれらしく受け取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として当事者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べき事柄であること③一般の人にまだ知られていない事柄であること④このような公開によって当該私人が現実に不快や不安の念を覚えたこと

（3）プライバシーと表現の自由

言論，表現等の自由の保障とプライバシーの保障とはいずれかが優先するという性質のものではなく，言論，表現等は他の法益すなわち名誉，信用などを侵害しないかぎりでその自由が保障されているものである」[10]．現在においてもこの判例が日本のプライバシー権を判断する根拠となっています．

現代の積極的プライバシー権では，他者が管理し保有する自己に関する情報の訂正，削除などを求めることもできる権利（自己に関する情報を制御する権利）とするという見方に変わっています．また日本では，過去に罪を犯した人に関する出版物の内容について賠償を認めた伊佐千尋「逆転」事件をめぐる判決があります．伊佐千尋のノンフィクション作品「逆転」で，実名を使用され前科を公表された男性Ａがプライバシー侵害にあたるとして，著者に慰謝料を請求した訴訟です．第１審判決（東京地方裁判所，１９８７年）は男性側の請求を一部認めました．控訴審判決（東京高等裁判所，１９８９年）はＡの主張するプライバシー侵害を認め，上告審判決（最高裁判所，１９９４年）はプライバシー侵害に関しては明言しなかったものの，原審を支持しました[10]．

２０１４年5月１３日，欧州連合（ＥＵ）司法裁判所（以下ＥＵ司法裁と略記）は，米検索大手グーグルに検索結果として表示された情報が，「プライバシー侵害にあたる」として削除を求めたスペイン人男性の要求を認める判断を下しました．あるスペイン人男性がグーグルで自分の名前を検索すると，社会保険料滞納のため不動産が競売にかけられたことを伝える１９９８年の新聞記事のリンクが表示されました．ＥＵ司法裁は，検索エンジンは基本的にプライバシー保護に責任があるとしました．そのうえで，たとえ検索表示が真実を表示していても，責任はあると述べました．利用者の知る権利とプライバシー保護は「公正なバランスを取るべきだ」とし，公人の場合は利用者の知る権利が優先されると判断しました．この事件はＥＵデータ保護規則案が適用される以前の（旧ＥＵデータ保護指令が適用される）事件であり，２０１３年に可決されたＥＵデータ保護規則案では，「忘れられる権利」は「削除を要求する権利」と名称に変更され，２０１５年に成立予定です．

米国は２０１２年に公開された「プライバシー権利章典」において，「Do Not Track」（行動ターゲッティング広告から追跡されることを拒む仕組み）などを用意し，利用者が自由にプライバシー保護を選択できるように環境整備を

行う事でサービスの利便性や経済活性化も担保する方式を採用してＥＵとは異なる方向になっています

日本では特定の情報へのリンク削除を求めた裁判で京都地裁では請求を棄却しました.２０１４年８月７日に，京都市の４０代男性Ｂが，検索大手ヤフー・ジャパンの検索サイトで名前を検索すると自分が迷惑行為防止条例違反容疑で逮捕された事実が表示されるとして，名誉毀損及びプライバシー侵害に基づいて同サイトを運営するヤフーに対して索結果の表示中止や慰謝料など約１１００万円を求めました．裁判長は「原告の逮捕事実は社会的な関心も高く，公共の利害に関する事実．原告の人格権が侵害されているとは言えない」として，男性Ｂの請求を棄却しました．ヤフー側は「検索サイトは社会インフラの一つ．検索結果の表示が違法なら，新聞の縮刷版を置いている図書館も違法になる」と反論していました．現在，控訴中です.

東京地裁では一部削除を命じる決定をしました.２０１４年１０月９日，米検索大手グーグルの検索サイトで男性Ｃの名前を検索した際，不適切な個人情報が表示されるのは人格権の侵害とする仮処分の申し立てに対し，東京地裁は「検索結果の一部はプライバシーとして保護されるべきで，人格権を侵害している」として検索結果の一部削除を命じる決定を出しました．地裁はこのうち，男性Ｃの名前が含まれるものなど１２２件について，男性の人格権を侵害していると認め，削除の仮処分を決定しました．グーグルは，地裁判断を尊重して仮処分に従う意向を表明しています.

プライバシー侵害が著しければ，人格権の侵害として，民事訴訟による削除請求となりますが京都地裁ではその請求が棄却されました．東京地裁の例では，人格権の侵害に対する仮処分を申し立てた例で，その申立てが認められ，削除の仮処分が決定されました．プライバシーでネットに残る個人情報は「忘れられる権利」が初めて保護されました.今後このような個別の問題に対して多くの判例を積み重ねていくことになります.

ＥＵ司法裁の訴訟も，日本の事例も，検索エンジンを提供する事業者が提訴された点では共通です．しかし，ＥＵ司法裁が，検索エンジンの社会的影響力の大きさから，情報の提供が適法であったとしても，リンクの削除をすべきと判断したのに対し，日本では，検索エンジンの社会的影響力の大きさを考慮した判断にはなりませんでした.

## 11. プライバシーポリシー（Privacy　Policy）

プライバシーポリシー は，インターネットのウェブサイトにおいて，収集した個人情報を保護するのか，それとも一定条件の元に利用するのかどう扱うのかなどを，サイトの管理者が定めた“規範”のことです．個人情報保護方針などともいわれています．

プライバシーポリシーは，利用規約の一部として記載している場合もあります．ウェブサイトによっては，この中に「第三者に情報提供する場合がある」と明記されている場合があります．このためサイト利用者は，個人情報をインターネットに送信する際には，プライバシーポリシーを熟読する必要がありますが免責事項には，「ウイルスなどの有害物が含まれていないこと，および第三者からの不正なアクセスのないこと，その他安全性に関する保証をすることはできません.」と記されていることがほとんどです．これは，インターネットの性質上，この責任まで負うと，大変な損害を被る可能性があるからです．ただし，これらの場合においても，必ずしも免責が有効であるとは限らず基本的にはウェブサイトの管理者の姿勢を宣言しているにすぎないこともあります．

Facebook や Google などが提供するサービスを利用するユーザーの大半は，例えば Facebook のデータの使用に関するポリシー「Facebook が受け取る情報の用途」は日本語で理解できても内容を１００％理解できているかは自信がないと言っており，これらのＷｅｂサイトが利用者の情報をどのように扱い，ほかのＷｅｂユーザーがどういった形で参照するのかについて書かれたプライバシーポリシーを読んでも基本的な内容を理解できていないことが，グローバルブランド戦略ファーム Siegel & Gale LLC が発表した調査報告からわかりました[11]．

最も厳格なプライバシー設定を有効にしても，Facebook サイトのユーザー・ネームは公開されたままであると知っていたユーザーは 30％にとどまっていました．政府文書や銀行カードの使用規定よりも難解で読んでもわかりませんが大半を占めています．

プライバシーマーク制度の場合は,民間の自主規制でプライバシーマークの認定を受けた付与事業者(一般財団法人　日本情報経済社会推進協会)は,「個人情報保護マネジメントシステム
（Personal Information Protection Management Systems：略称ＰＭＳ)」を確立し,「個人情報」を安全に管理する体制を整えています.

付与事業者はまず,「個人情報保護方針」を定め，この方針に基づきＰＭＳを推進するための社内の体制を整えます.

ＰＭＳの基本的な仕組みは,

① 作業計画を立てて（計画：Ｐｌａｎ),
② 「個人情報」の特定，規程などの作成とその運用，従業員の教育など実施していきます.（実施：Ｄｏ).
③ その運用状況を点検し（点検：Ｃｈｅｃｋ),
④ 課題を改善していきます.代表者は高い立場からＰＭＳ全体を見直します（見直し：Ａｃｔｉｏｎ).

以上から成る「ＰＤＣＡサイクル」によるものです[12].

ＯＥＣＤ（Organization for Economic Cooperation and Development：経済協力開発機構）が定めたプライバシー・ガイドラインは

① 「収集制限の原則」②「データ内容の原則」③「目的明確化の原則」
④ 「利用制限の原則」⑤「安全保護の原則」　⑥「公開の原則」
⑦ 「個人参加の原則」⑧「責任の原則」

など８項目からなる原則によって成り立ち，この原則は世界各国の個人情報保護やプライバシー保護に関する法律の基本原則として取り入れられています.

ＯＥＣＤでは，情報システムの基本概念として「ＣＩＡ（「機密性：Confidentiality」,「完全性：Integrity」,「可用性：Availability」，の欠如に起因する危害から情報システムを利用するユーザーを守ること」という定義を定め，セキュリティ文化の普及に向けて,情報システム及びネットワークのセキュリティのためのガイドライン(OECD Guidelines for the Security of Information Systems and Networks : TOWARDS　A CULTURE OF SECURITY)を承認しています[13].

## 12. おわりに

インターネットの普及にともない，これまでの利用者は情報の受信が主でしたが，ＳＮＳが爆発的に普及すると，利用者による発信情報が，インターネット上に流れる情報のかなりの部分を占めるようになりました.

そのような状況で，軽い気持ちで人を誹謗・中傷したり，意識しないで個人のプライバシーを表に出してしてしまったり，といったことが起きやすくなりました．そこには，ソーシャルネットワークが介在しており，ＳＮＳが問題となるケースが多くなっています.

狭義の「忘れられる権利」に関しては，日本でも司法判断が示され始めており，判例を積み重ねて徐々に運用や執行体制が整理されていくと思われます．プライバシーの問題は，素早い解決が求められ，不利益なプライバシーが表に出てしまったら，できるだけ早く差し止める必要があります.

一般に「忘れられる権利」を拡大解釈する傾向になっており，事業者はパーソナルデータを収集し,我々の日常はそれに振り回されることになります．こうした意識は，漠然としている状態というレベルから，具体的な懸念となりつつあります.

利用者からすれば，事業者の保有し管理する内容はできるだけ我々のことを忘れてほしいという思いをより強く抱く傾向にあります．議論の対象が少しずつ広義の「忘れられる権利」へと広がっていく可能性が高まっています.

今後日本でのプライバシーに関する判例を積み重ねる過程で多くの議論が必要となると思われます.

インターネット社会では善悪の判断と情報の信憑性の判断にはメディアリテラシーが必要です．社会生活の中でルールとマナーを守っていくことはもちろん,情報セキュリティ対策も情報漏洩などの事件の多さを見るにつけ，ますます重要さを増してきています.

社会的にもサイバーテロ対策が緊急の課題となっており，国際社会の中でもサイバー戦争の様相さえ帯びてきました．若い学生諸君には柔軟な発想で新しいセキュリティシステムを考案しながら，正義のハッカーとしての活躍が特に最近の公的機関でも求められています.

[文献及びホームページ]

1）長谷川欽一「応用倫理学としての情報倫理の営み」pp39-40
「技術倫理と社会　第 9 号」日本技術士会中部本部 ET の会　2014.4.12
2）山住富也『モバイルネットワーク時代の情報倫理』被害者・加害者にならないためのメディアリテラシー pp2-3, pp21-22, pp116-117, pp124-130　近代科学社
2013.3.31（初版 2009.9.30）
3）情報教育学研究会（IEC）・情報倫理教育研究グループ：「インターネット社会を生きるための情報倫理」pp66,pp94 実務出版　2013.3.31
4）日経パソコン　2013 年 4 月 8 日号の記事を参考
http://pc.nikkeibp.co.jp/npc/download/index.html
5）Facebook が買収！世界 No1 アプリ WhatsApp(ワッツアップ)とは？
On Device Reserch 社(英国)による 2013 年 9 月調査：https://ondeviceresearch.com/
6）「富山大サーバー 不正アクセス受け悪用される」
2015 年 6 月 7 日　朝日新聞デジタル
http://www.asahi.com/articles/ASH625DS6H62UUPI001.html
7）「125 万件の個人情報流出＝職員端末に．年金機構にサイバー攻撃」
2015 年 6 月 1 日及び 9 日：時事通信
http://www.jiji.com/
8）「個人情報の「同意なし転用」，拡大へ　改正案衆院通過」
2015 年 5 月 22 日：朝日新聞デジタル
http://www.asahi.com/articles/ASH5P7FYGH5PULFA02X.html
9）「相次ぐスマートフォンとプライバシーの問題-プライバシーって何だ？」
2012 年 1 月 26 日：日本経済新聞 Web 版
http://www.nikkei.com/article/DGXNASFK22013_S2A420C1000000/
10）田中秀和　「ビッグデータとプライバシー（忘れられる権利）」
日本技術士会中部本部技術者倫理研究会（第 38 回ＥＴ例会）2014.7.26
「技術倫理と社会　第 10 号」pp84 日本技術士会 ET の会　2015.4.11
11）グローバルブランド戦略ファーム Siegel & Gale LLC（以下シーゲルゲール、本社：米国ニューヨーク）が発表した調査報告
http://www.siegelgale.com
12）一般財団法人　日本情報経済社会推進協会
http://www.jipdec.or.jp/project/pmark.html
13）OECD Guidelines for the Security of Information Systems and Networks : TOWARDS　A CULTURE OF SECURITY）」
http://www.mofa.go.jp/mofaj/gaiko/oecd/privacy.htm