対策 8

個人情報と権利侵害

ビッグデータという言葉が数年前から使われ始めています。簡単に言うと大容量のデータを高速に分析できるようになったことから、色々なデータを集め、事業活動に有効利用しましょうということです。例えば、オンラインショップでの利用者の行動履歴を解析し、お薦めの広告を出したり、SNS の情報を解析し、知り合いかもしれない人を表示したり、普段の位置情報を解析し、その人の勤務先や自宅の天気や渋滞情報を案内したりと、あなたの位置情報、Web サイトでの検索・入力・言語変換の履歴、エラーが発生した際の情報など、様々な情報が収集され、サービスやアプリケーションの向上に役立てられるようになりました。

また、情報、画像、音楽、映像などのコンテンツを容易に検索しアクセスできるようになりました。さらにコンテンツをブログ、SNS などを通じ、簡単に発信・共有できるようになりました。

このようにビッグデータの収集が活発化し、コンテンツの発信・共有が容易になった近年、どのようにインターネットと付き合えばよいのでしょうか。ここでは、あなたの個人情報が悪用されたりプライバシーの侵害に遭わないために、また、あなたが誰かの権利を侵害したり、不法行為をしないために、何に注意すべきかを解説します。

個人情報と権利侵害に関する 4つのポイント

8-1 パソコンやスマートフォンで収集される情報を確認する

8-2 Webサイト閲覧履歴などの共有範囲を確認する

8-3 SNSでの個人情報公開に注意する

8-4 知的財産や個人情報などの権利や法令を意識する

8-1 パソコンやスマートフォンで収集される情報を確認する

パソコンやスマートフォンなどで使う共通の Google アカウント、Apple ID、MS アカウントなどでは、利用履歴などの情報が活発に収集されており、利用者が提供したくないと感じる情報も収集されている可能性があります。Android、iOS、Windows 10 以降などでは、初期設定のまま提供者の推奨設定を選択すると様々な情報が収集の対象となります。プライバシー設定をよく確認し、自分が提供してよいと思える情報に限定するようにしましょう。

各 OS のプライバシー設定

■ **Windows 10**
［設定］›［プライバシー］

■ **macOS**
［システム環境設定］›［セキュリティとプライバシー］›［プライバシー］

■ **iOS**
［設定］›［プライバシー］

■ **Android**
［設定］›［Google］›［個人情報とプライバシー］
［設定］›［アプリ］›（各アプリを開く）›［許可］

8-2 Webサイト閲覧履歴などの共有範囲を確認する

Web ブラウザによる Web サイトの検索、閲覧、Web サービスの利用は、金銭管理に関わる情報、業務情報、個人の趣味趣向や思想など、利用者の業務やプライバシーにかかわる情報を多く含んでいます。

他の利用者と共有するパソコンにおいては、Web サイト閲覧などの履歴情報だけでなく、認証情報（ログイン中の状態）もパソコン上に残ることがあり、**他人に履歴情報を閲覧されるだけでなく、利用していた Web サービスなどにログインされてしまう危険性があります。こういった情報が残ることを防ぐため、共有するパソコンで、Web サービスを利用する際には、必ず Web ブラウザのプライベートブラウジングを利用しましょう**（Internet Explorer 11・Edge は InPrivate ブラウズ、Chrome はシークレットモード、Firefox はプ

ライベートウィンドウ、Safari はプライベートブラウズとそれぞれ名前が違います)。そのうえで利用後には、必ずログアウトし、Web ブラウザを終了するようにしましょう。

また、Edge と MS アカウント、Chrome と Google アカウント、Safari と Apple ID などクラウドサービスのアカウントと連携可能な Web ブラウザは、Web サイト閲覧履歴、ブックマーク、ID・パスワードなどをクラウド上に預けて（保存して)、どのデバイスからでも利用可能にしている一方、閲覧履歴などをビッグデータとして活用する場合もあります。Web ブラウザやクラウドサービスのアカウントのプライバシー設定をよく確認し、パソコン・スマートフォン・タブレットなどの機器より外に出したくない項目をオフに設定しましょう。

8-3 SNSでの個人情報公開に注意する

SNS の使い方やモラルについては、学生向けの「SNS 利用にあたって知ってもらいたい５つのこと」（SNS ガイドライン）が大変参考になりますので、一度は読んでおくようにしましょう。

SNS は、自分の個人情報が悪用されるという観点、さらに（あなたが投稿した情報や SNS のつながりなどで）あなたの友人の個人情報が悪用される可能性があるという点で注意が必要です。特にコメント、アップロードした写真などに写り込んだ背景など、複数の情報を組合わせて個人が特定される可能性があります。**１回の投稿では個人を特定することはできなくても、投稿を組合わせて個人が特定可能となるケースがあることに注意しましょう。**

また、意図せず（主に SNS やサービスへの規約や技術的理解不足から)、個人情報を公開してしまうケースも増加しています。

意図せず個人情報を公開してしまう例

- 公開範囲を確認せずに使っている
- 公開範囲を誤って設定している
- 写真や投稿に位置情報が含まれることに気づいていない
- あなたの投稿を共有した友人が再共有・公開する
- SNS 運営者が投稿内容などの情報を収集し、目的外利用や第三者提供することを確認していない

こういった情報を悪用して個人を特定し、標的型攻撃メールや詐欺をおこなうより巧妙化した手口が増加しています。このような巧妙化した手口を見破ることは難しいため、**SNS の機能、公開範囲、サービス利用規約やプライバシーポリシー（対策 9-2「個人情報の取扱いについて確認する」参照）などをよく確認し、意図しない個人情報の公開を避けましょう。**

参考：立命館大学　SNS 利用にあたって知ってもらいたい 5 つのこと、SNS ガイドライン
http://www.ritsumei.ac.jp/rs/sns/

参考：総務省　国民のための情報セキュリティサイト「SNS 利用上の注意点」
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/enduser/security02/05.html

参考：日経 BP　SNS の落とし穴：こんなはずじゃなかった！ SNS で個人情報がダダ漏れ、取り返しのつかないことに
http://www.nikkeibp.co.jp/article/matome/20131125/374827/

解説⑫

位置情報取得機能や画像に埋め込まれる位置情報

位置情報を取得可能な機器（携帯電話、スマートフォン、一部のデジタルカメラ）で写真を撮った場合、画像にはその写真を撮った位置情報が埋め込まれます（ジオタグと呼びます。下図は iPhone のカメラが埋めた情報を Windows 上で確認したもので、緯度・経度情報が表示されています。）。緯度・経度情報があれば、地図アプリなどで簡単に場所が判明します。

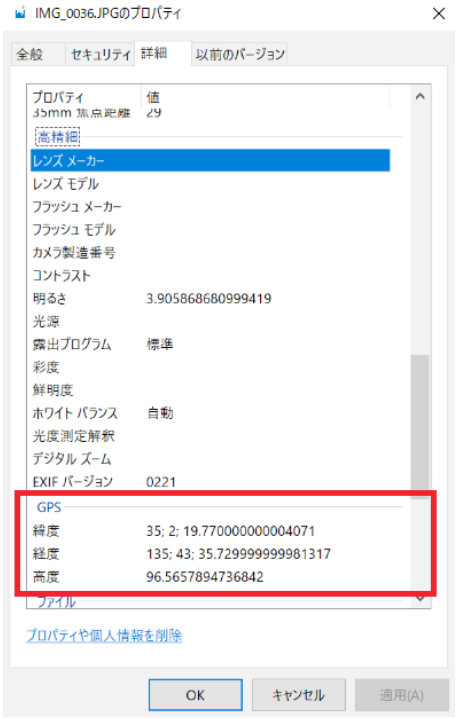


図 23　iPhone で撮影した写真のプロパティ

また、Twitter の SNS アプリなどでは、テキストの投稿なども位置情報公開につながるケースがあります。写真を撮影した場所や投稿した場所、投稿の内容を照らし合わせることで、それがどういった場所なのか（自宅など）判明することがあります。

＜事例「自宅で猫の写真を撮って投稿」＞

A さんは、SNS で本名を公開しています。ある日、A さんは自宅で猫をスマートフォンで写真を撮って、SNS で公開しましたところ、数日後から A さん宛に架空請求などの郵便が届くようになりました。

さらに行動解析などによって自宅や職場が推定されることがあります。SNS 利用では、特に位置情報に気を付けましょう。

Tips 10

秘密の質問と SNS

対策 4「メール」では、標的型攻撃メールや詐欺の下調べとして、利用者本人に関わる様々な情報が掲載される SNS が利用されるケースがあることを紹介しました。似たような考え方で「秘密の質問」と SNS で気をつけるべきことがあります。

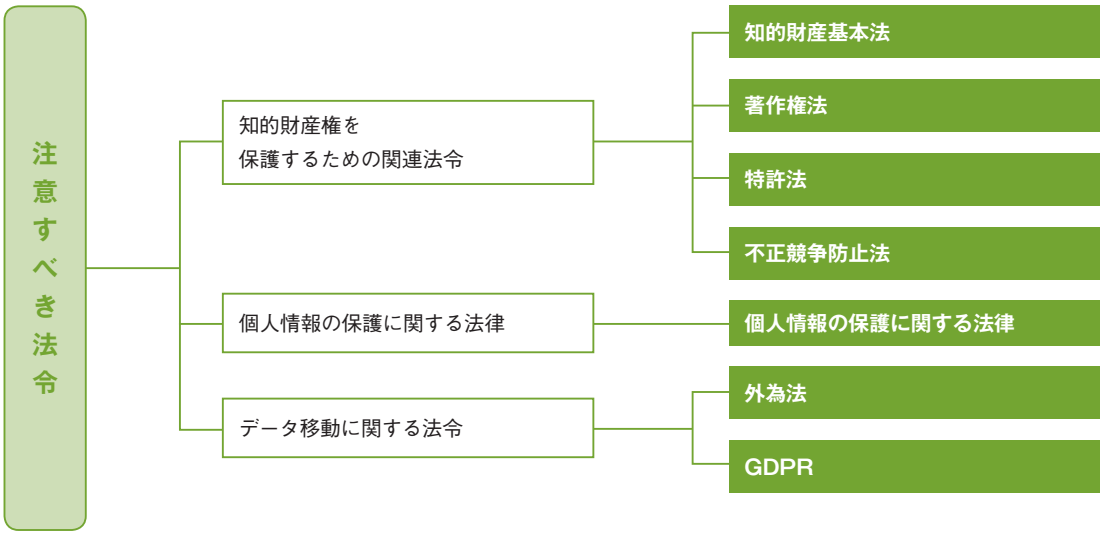
「秘密の質問」とは、パスワードを忘れた利用者が再発行や通知を受ける手続き時に、ユーザー登録時などに予め決めておいた本人しか知らない質問を入力することで本人確認をする機能です。「母の旧姓は？」「好きな食べ物は？」「ペットの名前は？」などの質問があります。この秘密の質問は、効果のある本人確認方法のように見えますが、正直に答えると非常に危険です。なぜなら、身近な人が知っている情報であったり、**SNS で様々なことを公開しているとより推測が容易になったり、秘密の質問の答えそのものを意識せずに公開している場合があるからです。**このように、容易に ID・パスワードを窃取される恐れがあることから、認証の仕組みとして「秘密の質問」を廃止する呼びかけが広まっています。

「秘密の質問」の答えを登録する場合には、推測される可能性のある正解を使わないようにしましょう。

参考 IPA「その秘密の質問の答えは第三者に推測されてしまうかもしれません」
https://www.ipa.go.jp/security/txt/2015/07outline.html

8-4 知的財産や個人情報などの権利や法令を意識する

インターネットを利用する上で意識すべき法令は、下図に示すような「知的財産権を保護するための関連法令」「個人情報の保護に関する法令」「データ移動に関する法令」の 3 つです。



引用元：図解入門ビジネス　最新 ISO27001 2013 の仕組みがよ～くわかる本

図 24　意識すべき法令

第一に「知的財産権を保護するための関連法令」についてです。インターネットが身近になったことで、画像、音楽、動画、文書などに代表されるコンテンツの入手、複製、公開、共有が非常に容易になりました。こういったコンテンツには、著作権に代表される知的財産権があり、法令により保護されています。著作権法では「学校教育の目的上必要と認められる限度において」「営利を目的としない」など、授業や教材への著作物の利用について寛容な部分はありますが、解釈が間違っていたり、使用許諾契約により利用範囲を制限されていたりするケースもあります。著作権だけではなく産業財産権（商標権、特許権、実用新案権、意匠権）、営業秘密など知的財産権全般についても配慮が必要です。例えば、本人承諾を取っていない誰かの顔が映り込んだ写真や映像をインターネットで公開または共有すれば、権利侵害となります。

第二に「個人情報の保護に関する法令」も多くの個人情報を扱う本学園にとって重要です。「学校法人立命館個人情報保護規程」（以下、個人情報保護規程）では、教職員には個人情報を適正に管理することが責務とされており、個人情報保護規程、個人情報の保護に関する法律（以下、個人情報保護法）およびガイドラインをよく理解した上で、教育研究活動・管理運営などの業務において、遵守するようにしましょう。

第三に「データ移動に関する法令」は見落としがちですが、注意してください。重要なものは、「外国為替及び外国貿易法」（以下、外為法）と「General Data Protection Regulation」

（EU 一般データ保護規則、以下、GDPR）の２つです。外為法は、安全保障輸出管理観点から、武器や軍事転用可能な技術が特定の地域に渡らないようにするためのもので、情報はインターネットを通じ、簡単に国境を超えるので注意が必要です。GDPR は日本の個人情報保護法と同様に、欧州経済領域（EEA 域内）における個人情報保護のための法律で、日本よりも厳格なルールとなっています。EEA 域内に所在する個人から越境して個人情報を取得するケース、および EEA 域内から個人情報を EEA 域外に越境するケースにおいて、GDPR の基準を満たす必要があるので注意が必要です。

さらに、法令には明記されていませんが、プライバシー権や肖像権も過去の判例に基づき憲法 13 条の幸福追求権や個人の尊重から人格権の一部として認められており、侵害すれば不法行為となります。情報（ここではデータやコンテンツ）によっては、秘密保持契約（NDR）や使用許諾契約などで法的に規制される場合もあります。

権利侵害や不法行為を起こさないために、まずは、**インターネットでデータやコンテンツを活用する際には、様々な制約・制限によって縛られるということを意識して、どの範囲で使ってよいのか、誰に見せてもよいのか、といった制限事項を把握しましょう。**

そして、**複製、公開、共有が容易なインターネットの世界において、前述の情報に課せられた制限事項に合わせた適切なアクセス権の設定（対策６「アクセス権の管理」参照）を実施する**ことで、誤ってインターネット公開したり、共有により情報が漏えいするような事態を避けましょう。

参考：一般社団法人 日本著作権教育研究会　著作権 Q & A
http://jcea.info/Q&A.html

参考：社団法人私立大学情報教育委員会「教員のための個人情報活用ガイドライン」
http://www.juce.jp/kojin_joho/
※ 2017 年度改正前のガイドラインです

参考：個人情報保護委員会
https://www.ppc.go.jp/

解説⑬

国境を越えてはいけない情報

情報が国境を越えることを規制する代表的な法令に「外為法」と「GDPR」があるのは前述の通りです。物理的なものであれば、それが国境を越えることはイメージしやすいのですが、インターネットの世界で情報を「持ち出してはいけない」「国境を越えてはいけない」という状況は少しイメージしにくいかもしれません。

例えば、「外為法」により規制対象となる情報を、誤ってインターネット公開する、特定地域からのアクセスを許可する、特定地域国籍を持った相手に共有した場合、**学内に設置したサーバーであっても規制対象となります**。逆にクラウドサービスなどでデータ保管場所（クラウドサービスのデータが実際にあるデータセンター等の場所）が特定地域にあったとしても、特定地域からのアクセスが規制されていれば、問題ありません。

一方、「GDPR」では、EEA 域内に所在する個人に関するあらゆる情報を域外の「十分性認定（十分なデータ保護レベルを確保していると EU が認定すること）」を受けていない第三国に移転することが制限されています。日本は 2018 年現在、この「十分性認定」を受けていないため、EEA 域内で収集した EEA 域内に所在する個人の情報を日本（学内や日本のデータセンターを使うクラウドサービス）に持ち込む場合や、EEA 域内を含む個人から情報を収集する場合には、GDPR の基準を確認し、対応する必要があります。しかし、Google、Amazon、Microsoft などの契約条項を提供するサービス上で情報を管理することは可能です。詳しくは各サービスの FAQ をよく読みましょう。

参考：立命館大学の安全保障輸出管理関連の資料・様式等
http://www.ritsumei.ac.jp/research/member/study_ethic/se15.html/