Ｐマークニュース ＜２０１９年爽秋号＞　Vol.　２９	（株）トムソンネット Ｐマークコンサルティンググループ

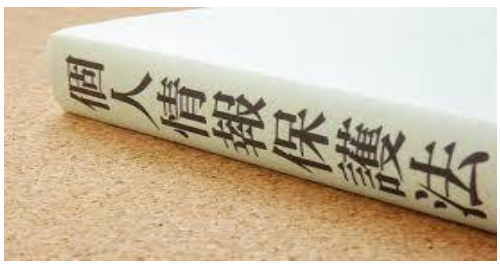
１．個人データ利用の情報提供サービスの拡大と規制

―リクナビ「内定辞退率予測」への個情委「是正勧告」の教訓―

個人情報保護委員会がはじめて、法に基づく「是正勧告」を行いました。(2019.8.26)
個人情報の利活用に関する違反です。
また、大企業での個人情報利活用(GAFA 対応でもあるが)について公正取引委員会は「優越的地位の乱用」を個人情報保護にも適用し、個人データ利用「違反」に対して、監視・抑止力を強める指針案を公表しました。(2019.8.29)
2020 年個人情報保護法改正の論議もあります。

個人データを利用した情報提供サービスの拡大と規制の論議を追ってみました。

オンライン・ショッピング・モール、アプリケーション・マーケット、検索サービス、コンテンツ（映像、動画、音楽、電子書籍等）配信サービス、ソーシャル・ネットワーキング・サービス（ＳＮＳ）など、個人データを利用した各種情報提供サービスは、革新的なビジネスや市場を生み出し続け、その恩恵は、中小企業を含む事業者にとっては市場へのアクセスの可能性を飛躍的に高め、消費者にとっては便益向上につながるなど、経済や社会にとって、重要な存在となっています。



そんな中、個人情報保護委員会(以下個情委)は、はじめての「是正勧告」をリクルートキャリアに対して行いました。(2019.8.26)

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が、企業向けサービス「リクナビ DMP フォロー」で、過去のリクナビユーザーの行動履歴などを分析して予測モデルを作成し、リクナビや提携就職情報サイトにおける応募学生の行動ログと照合することで内定辞退率をスコア化し、契約企業へ提供していました。

データの提供にあたり一部で同意を得ないままデータを提供していたことが判明し、個人情報保護委員会により指導を受けました。個人情報の「提供」に際しての保護法違反です。

同委員会はサービスを利用していた 38 社にも個人情報の扱い方で不備がなかったか調査する方針といわれています。

また、公正取引委員会は、プラットフォーマーと呼ばれる IT 企業を独占禁止法で規制するための指針案を公表しました。(2019.8.29)

情報量や交渉力で強い立場にある IT 企業が個人のデータを吸い上げる行為を独禁法違反の恐れがあると明記し、指針案では個人情報の取得や利用で法律違反の恐れがある例を大きく 4 つに分類し示しました。

①利用目的を消費者に知らせずに個人情報を取得すること。

（想定例）個人情報を取得するに当たり，その利用目的を自社のウェブサイト等で知らせることなく，消費者に個人情報を提供させた。

②利用目的の達成に必要な範囲を超えて、消費者の意に反して個人情報を取得･利用すること。

（想定例）サービスを利用する消費者から取得した個人情報を、消費者の同意を得ることなく第三者に提供した。「リクナビ」問題など

③個人情報の安全管理のために必要かつ適切な措置を講じずに、個人情報を取得・利用すること。

（想定例）個人情報の安全管理のために必要かつ適切 な措置を講じずに、サービスを利用させ、個人情報を提供させた。

④自己の提供するサービスを継続して利用する消費者に対し、消費者がサービスを利用するため の対価として提供している個人情報等とは別に、個人情報等の経済上の利益を提供させること。

（想定例）提供するサービスを継続して利用する消費者から対価として取得する個人情報等とは別に、追加的に個人情報等を提供させた。

公正取引委員会は、独禁法上の**「優越的地位の乱用」**として禁じる。これまでは企業間の取引のみに適用してきたが、企業と個人の間のデータのやり取りにも適用できるよう考え方を整理しました。個人情報は個人情報保護法でも規制があります。ただ急速に成長するプラットフォーマーが利用者個人との力の差を利用して強制的に個人情報の提供を同意させたり、不要な情報を吸い上げたりする行為は、独禁法での規制も必要と判断したものです。

本人に利用目的などの説明が不足したまま個人情報を外部に提供していた就職情報サイト「リクナビ」も、規制の対象になり得るという見解が大勢です。学生の「取引必要性」に乗じて、「優越的地位」を使った事例と言えそうです。GAFA など大規模プラットフォーマーの規制だけでなく、社会に影響を与えうる大企業でも、「取引必要性」が認められ「優越的地位の乱用」があれば規制の対象となるのです。

保険会社と代理店の間で、契約者データを利用した情報提供サービスが行われ、「優越的地位の乱用」と認められれば、規制の対象となり得ることにも留意する必要があります。

一方、個人情報保護法の 2020 年改訂原案では、「**利用停止等**」に関して、「利用停止等に関して、個人の権利の範囲を広げる方法について検討する必要がある。一方、消去については、例えば、完全に消去してしまうと、過去に消去請求をした者であるという事実を含め、当該本人に関する情報を一切保有しないことになり、その後、再び当該本人の個人情報を取得した場合に当該個人情報を利用することの可否等の消費者の利便や実務上の論点もある。利用停止等については、**個人の権利を保護していく観点から**どのようにすれば一定の対応が可能か、**企業側の実態も踏まえつつ、具体的に検討していく必要**がある。」としています。

個人データを利用した情報提供サービスについては、「データ利活用に関する施策の在り方」に関してとして、**ターゲティング広告をめぐる対応の在り方も含めて、「**技術の進展に伴い、データを活用した新たなサービスが次々と生まれてきており、その中における個人情報の取扱いについては、**実態を踏まえて対応**していくことが重要である。このような取扱いについては、個人情報保護法に直接関係する論点もあれば、同法とは直接は関係しない論点もあり、その実態に応じて**論点も多様である**ことが想定される。委員会としては、まずは法令の規定に即し対応を行っていくこととなるが、その際、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という同法の趣旨を踏まえ、検討することが重要である。」とし、やや具体性に欠けており、公取委のような明確な改革案ではなくなっています。

公正取引委員会の指針について、「同意しても後から理解していなかったと言い出す非合理な個人を相手にビジネスをすることの怖さ」のあるわが国でのビジネス実態を憂う識者の意見があります。

また、公正取引委員会が「大手企業が強い立場を利用して個人情報を同意なく使うと『独占的地位の乱用』に当たる」と規定することについて、経団連は「独占的地位にあたるかどうかの判断は抑制的であるべきだ」とコメントしています。(2019.10.16)

「リクナビ」問題で一層論議を呼んでいる個人データを利用した情報提供サービスの拡大と規制の結論が、2020 年どうまとまるか注目されます。

２．保険代理店様における個人情報保護への取り組み（５）

昨年の爽秋号以来、掲載をお休みしておりました「保険代理店様における個人情報保護への取り組み」の復活です。今回は、ＥＩＣ保険エージェンシー株式会社様の取り組みです。

今年の３月にＰマークを取得された同社において、Ｐマーク運営を牽引されておられます取締役管理部長滝沢様に、Ｐマークの取得及び運営についてご意見等をお伺いしました。

Ｑ１．保険代理店として、Ｐマークを取得して良かったと思う点があればお教えください。

Ａ：当社ではＰマーク取得を目指して、個人顧客のみならず、法人顧客も含めて「顧客情報の漏えい等を防止する」との観点でＰＭＳ構築に取り組んだため、改正保険業法で求められている「顧客情報管理態勢」について、改めて社内の確認、チェック、見直し等を行うことができ、更なる態勢の強化に繋がったと思います。また店主や態勢整備・コンプライアンス推進責任者のみならず、毎月の点検等を通じて各部門責任者や各社員が「自分事」として個人(顧客)情報管理・保護を意識する取り組みになったと感じています。

対外的には、Ｐマークの取得により、お客さまの大切な情報を多く取り扱う保険代理店として、お客さまに安心、信用、信頼していただくための１つの要因になればと期待しています。

Ｑ２．Ｐマークを取得する「前」と「後」では、社内の個人情報の取扱いに対する「意識」の変化はありましたか。

Ａ：Ｐマーク取得前は、ミーティングや各種点検等で、全役職員が個人情報の取り扱いについて注意、確認する機会を設けていましたが、Ｐマーク取得後は、年一回の教育研修、全員が毎月実施している「ＰＣ簡易セキュリティ診断」や、各部門責任者による「運用点検チェックリスト」など、継続的な取り組みを通じてＰＭＳの重要性を意識する（できる）環境、体制が更に整備されたことで、全役職員の個人（顧客）情報の取り扱いに対する「意識」は変わってきたと感じています。

また、Ｐマーク取得に向けて書類のファイリングや保管方法等を見直したことによって、「オフィスが綺麗になった。」とのお声をいただいたことが何度かありました。

その他、名刺に印刷したＰマークや、ホームページ、店頭に掲示した「登録証」等を目にすることによって、社員各々が「漏えい事故を起こしてはいけない」「注意しなければ…」との意識が、少なからず根付いてきていると感じています。

Ｑ３．今後、Ｐマークを取得するか否かで悩まれている代理店に何かアドバイスはありますか。

Ａ：上記１．にも示したとおり、Ｐマーク取得を目指すことにより、各社員、部門責任者が各種点検等を通じて、「自分事」として個人（顧客）情報管理・保護に取り組む良いきっかけになったと思いますし、目的を問わず「ＰＤＣＡ」を実践する内体制構築の一助になったと感じています。

３．事例に学ぶ：ブリティッシュ・エアウェイズ（BA）に 250 億円の制裁金

事例シリーズの第 6 弾になります。今回は個人情報の流出で莫大な制裁金(罰金)が科せられた例を取り上げます。

本年(2019 年)7 月に「英国の情報コミッショナー（ICO）が、英航空大手 British Airways に対して、1 億 8340 万ポンド（約 250 億円）の罰金が科せられた」と報道され、世界中を震撼させました。目下同社から異議の申立を行っているようですが、以前の P マークニュースでも紹介されている欧州における GDPR(一般データ保護規則)に対する違反です。

この事件は一見すると国際的な、或いは欧州で個人情報を扱う大企業でのみ起こり得るように思われますが、罰金はさておき事象としては国内の一般企業においても発生する可能性があるものです。又、システム不備が法によって裁かれた希有な例に当たります。

原因は、以前から喧伝されている〝Web サイトの脆弱性〟を突かれたものです。その中でも**〝フォームジャッキング〟**によるものと言われています。利用者が端末(パソコン、スマホなど)から入力したデータが、そっくり犯人のサーバに転送されました。

（1）Web サイト脆弱性のパターン

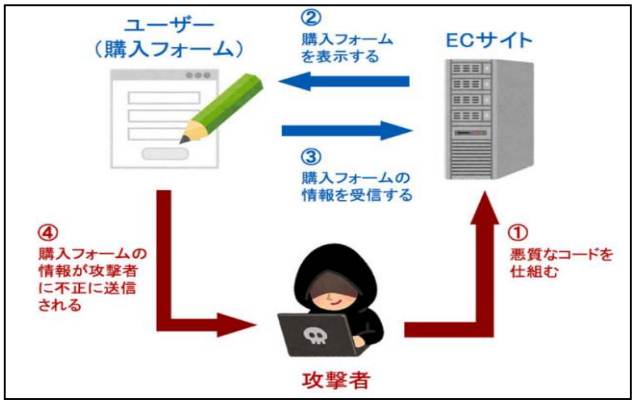
Web サイト(ホームページ)に〝脆弱性〟を持っていた場合、別の画面(正規の画面と酷似)が表示されたり、お客さんが入力したデータを悪用されたりします。パターンとして 2 つが挙げられ、それぞれに対策を講じる必要があります。

①Web アプリケーションのプログラミングに起因するもの

入力されたデータのチェックが不完全なために発生するもので、代表的なものに SQL インジェクションとクロスサイトスクリプティング(XSS)、OS コマンドインジェクションがあります。対策は偏に〝強靭な〟Web アプリケーションにすることです。

IPA((独)情報処理推進機構)では、指針として「安全なウェブサイトの作り方」などを公開し、強靭なアプリケーションとするためのプログラミング技法を示しています。

フォームジャッキングのイメージ



(株)シーズ・クリエイト HP から引用

Web アプリケーションの開発を委託する場合には、最低限 IPA の指針を盛り込んでいることを検収条件に入れるようお勧めします。

この範疇には、Web アプリケーションのベースになっている各社のソフトウェア製品も含まれます。プログラミングの問題ではありませんので、IPA の指針をユーザ企業で盛り込むことはできません。Java や WordPress、EC-CUBE、CRM(Salesforce 他)などが該当し、アンテナ高く頻繁に情報収集に努めタイムリーにバージョンアップすることが重要な対策になります。

②Web サイトの防御の甘さに起因するもの

Web サイトに入力画面がなく、又アプリケーションが強靭であっても、それを改ざんされたりデータの横取りをされたりすると身も蓋もありません。加えて、正規のサーバ（Web アプリケーション）にも入力データはもたらされますので攻撃されたことが発覚するのに時間がかかります。

〝フォームジャッキング〟〝スキミング〟などの事例があり、BA 社の事案はチケットの申込みデータが 2018 年 8 月 21 日～2018 年 9 月 5 日の間に予約入力した個人情報と決済情報が盗まれた、と言うものです。BA 社の発表では、影響を受けた顧客は 24 万 4000 人だったとしていますので、ベネッセ社の約 3,000 万人の事件に比して制裁金が大すぎるとの意見もあるようですが。

この脆弱性は、フォームジャッキングだけではなく色々な派生事象を現出しますので、対策については次項で検討したく思います。

（2）Web サイト改ざんの予防と検知

Web サイト(ホームページ(HP)やアプリケーションプログラムなど)が改ざんされると、ハンドルを失ったクルマのようにどんなことが起こるか見当が付きません。できる限りの予防措置と万一の場合を想定しておくことが肝要です。

①改ざんへの予防措置

とにもかくにも管理者のパスワードをできるだけ文字数を多くし、文字種も大小の英字と数字に特殊記号を混ぜることがベストです。ウィキペディアによると、パスワードの解読時間は

・英小文字のみ 8 文字⇒5 秒
・数字 2 つを最後に追加して 10 文字⇒1 日
・数字ではなく英小文字を 4 文字最後に追加して 12 文字⇒4 週間
・追加する 4 文字のうちの 1 文字を大文字にして 12 文字⇒300 年

とのレポートがあります。〝**英数字と特殊記号で 12 文字**〟以上が推奨されます。

なお、パスワードはホームページについてだけではありません。「ftp パスワード」も同様にし、可能であれば「telnet」の使用も禁止の設定にすべきです。

②改ざんの検知

Web サイト()が改ざんされていないかどうかは、実際に開いてみるか無料診断サービスのサイト(例：https://check.gred.jp/)に HP の URL を入力することで確認できます。

ただ、HP のページ数が多い場合には手間が大変で検知ソフトを利用せざるを得ないでし戻す機能を持つ製品もあります。購入する方法(オンプレミス)もありますが、月々数万円の費用を支払うクラウド型のサービスが主流になってきています。

③改ざんの事後処理

改ざんされた場合、HP を閉鎖し原本から元に戻すしかありません。原本の回復ソフトを利用していない限り手作業になります。その際、往々にして〝属性〟を間違え HP が開かないなどのトラブルも起こり勝ちです。事前に練習しておきましょう。

（3）「WAF」のお勧め

Web サイトが改ざんされると、多くの場合日数がかかります。一方、**「WAF」(Web Application Firewall)**をセットアップすれば悪意のある入力データからほぼリアルタイムで防衛できます。

WAF は IPA でも推奨しているセキュリティ対策で、〝意味〟を理解して不正メッセージを遮断します。例えば、ログイン画面に対する ID やパスワードに相応しくない入力データなどです。SOMPO リスクマネジメント(株)などがサービスを提供しています。又、プロバイダによってオプション機能になっている場合がありますので、機能的に多少不満があったとしても直ぐに〝有効〟にしましょう。

（4）まとめ

Web サイトの改ざんは顧客からの信頼失墜やホームページの閉鎖などを惹起します。それればかりではなく踏み台にされ、取引先への標的型攻撃や DDoS 攻撃の一端を担い多額の賠償金を請求されることにもなりかねません。

取り敢えずはこまめに、或いは無料サービスなどで自社のサイトを点検するようにしてはいかがかと思います。

なお、「事例に学ぶシリーズ」ではこれまでに以下を採り上げてきました。

P マークニュースのバックナンバーは弊社 HP からご覧いただけます、

回数	事例のテーマ	掲載
第１回	技術的安全対策で十分か ～日本年金機構個人情報漏洩事案～	2018 年陽春号
第２回	「認識」に漏れはないか　～日本年金機構入力ミス事案～	2018 年爽秋号
第３回	「危険メール」の防御策 ～標的型攻撃、BEC 等に備えて～	2019 年新春号
第４回	個人情報の紛失対策　～書類の事故等に備えて～	2019 年陽春号
第５回	テレワークに伴うリスク対策	2019 年盛夏号

４．お知らせ（大募集！）

2012 年の 10 月に創刊しました当 P マークニュースは、みなさまのご支援に支えられ、お陰様で、次号（2020 年新春号）で創刊 30 号を迎えます。

創刊 30 号を迎えるに当たり、弊社では、P マークニュースがよりみなさまに寄り添い、お役に立てる情報源となるべく、読者の**みなさまからＰマークニュースに対するご意見やご要望を大募集致します。**

「あの記事はよかったよ！」、「こんな記事が読みたいのだが・・・」等、是非、日頃のお気づきの点を下記の連絡先にお寄せ下さい。宜しくお願い申し上げます。

以上

弊社へのご連絡・ご相談は下記で承っています。ご気軽にどうぞ！
Ｐマークニュースに対するご意見、ご要望もお願い致します。

連絡先　　**株式会社トムソンネット**　(http://www.tmsn.net/)
〒101-0062 東京都千代田区内神田駿河台４－６　御茶ノ水ソラシティ１３階
電話　03-3527-1666　　FAX03-5298-2556
担当:　岩原 秀雄（Mail：iwaharahi1017@tmsn.net）　　平泉 哲史（Mail：s.hiraizumi@tmsn.net）
本間 晋吾（Mail: s.honma@tmsn.net）