Ｐマークニュース ＜２０１９年盛夏号＞　Vol.　２８	（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．SNS の利用拡大と個人情報

インターネットを使って人々が交流できるサービスの SNS は、個人間の情報の発信・共有・拡散といった機能に重きを置いており、その個人情報は、事業の用に供する個人情報保護法の規制対象外ですが、「社内 SNS」などとして、利用拡大が進んでいます。

その利用拡大とともに、個人情報保護法に新たな課題を投げかけています。以下では、GAFA（Google、Amazon、Facebook、Apple）に対する規制強化の動向とともに、SNS の個人情報保護に係わる課題を洗ってみます。

（１）SNS（Social Networking Service）って？

ブログ・電子掲示版なども広い意味では SNS に含まれますが、ここではスマホとともに広まり、「情報の発信・共有・拡散」といった機能に重きを置いた以下の WEB サービスをさします。「Facebook」（フェイスブック）、短いつぶやきを投稿・共有する「Twitter」（ツイッター）、写真の投稿・共有を中心とする「Instagram」（インスタグラム）、ビジネス・職業上の繋がりに絞った「LinkedIn」（リンクトイン）、更に「mixi」（ミクシィ）や「LINE」（ライン）、料理レシピ投稿サイトの「Cookpad」（クックパッド）等です。

これらのサービスには、人と人との社会的な繋がりを維持・促進する様々な機能を提供する会員制のオンラインサービスや、友人・知人間のコミュニケーションを円滑にする手段や場を提供したり、趣味や嗜好、居住地域、出身校、あるいは「友人の友人」といった共通点や繋がりを通じて、新たな人間関係を構築する場を提供するサービスなどがあります。

その個人情報取扱いで、ここで留意すべきは、SNS で発信され、共有される個人情報があったとしても、個人情報取扱事業者に該当しない個人が取扱う場合は、**個人情報保護法（以下保護法という）は適用されず、保護法に基づく義務を負わないことです。**例えば「友人が SNS で私の個人情報を公開して困っている。」としても保護法の違反ではないなどです。

また、事業者が SNS を通じて得た個人情報は、「第三者による提供」情報とは言えず、「提供受け」の保護法上の義務を負いません。SNS では、原則本人が提供の同意をしたうえで発信しているからです。このことは、事業者にとって、新規顧

客情報の取得が行いやすい手段になるとも言えそうです。取得後の利用目的の明示通知などは、保護法に基づき必要です。

（２）SNS で扱う「個人関連情報」

SNS では、クッキーなど端末識別情報・位置情報が発信され、SNS 事業者には、それ等の情報と検索履歴・閲覧履歴を含むログ情報が蓄積されます。

これら情報は「個人情報」の定義には当てはまらず、いわば「個人関連情報」です。これら情報を利用して、**「ターゲティング広告」**がなされています。サイト訪問時に、クッキーや広告 ID 等と結び付いた利用者のサイト訪問履歴等が取得され、広告配信に利用されます。ターゲティング広告では、PC やスマートフォン等のブラウザごとのクッキー上に発行される ID に紐付いて蓄積される情報(サイト閲覧履歴等)や、スマートフォン等の OS が発行する広告識別子に紐付いて蓄積される情報が使われることが多いとされます。また、最近は、スマートフォンの普及等により、ウェブ上の検索履歴や閲覧履歴のみならず、位置情報を含めた広い意味での行動履歴が利用され得る状況にあります。

従って、ターゲティング広告は、企業にとって有用であると同時に、利用者にとっても興味関心のある広告に接する機会が増えるという利点があります。しかし、ターゲティング広告を巡っては、以前から、消費者からプライバシーに対する懸念等が指摘されてきています。

例えば、知らないうちにデータが収集されること、個人の詳細なプロファイルが集積されることによるリスク、センシティブ情報が悪用されるおそれなどです。

更に、蓄積された個人情報を個人ごとに「プロファイリング」し、AI 技術も加わり**「スコアリング」**に利用する段階になっています。日本の「J スコアー」や中国の「芝麻信用」などが該当します。「芝麻信用」は、アリババグループの信用管理システムですが、「ネット上の資産や取引状況」「SNS の交友関係」などから信用度をスコア化し、予約ホテルの部屋のグレード等も決まると言われています。

（３）SNS「個人関連情報」の欧米での扱い

EU は、2018.5.25 に施行された GDPR「General Data Protection Regulation」（日本語訳：一般データ保護規則）によって、「位置情報、メールアドレス、オンライン識別子(IP アドレス クッキー)」は個人情報と定義し、更に日本では定義に含まれていない「クレジットカード情報、履歴データ（個人が含まれていない場合でも該当）」も個人情報としており、これらの個人情報の取扱いについて次の**個人の基本的権利**が規定されています。

・制限権
・忘れられる権利
・データポータビリティの権利
・異議を唱える権利(プロファイリングに異議を唱える権利)
・自動的処理のみによる意思決定に服さない権利

です。

GDPR の「説明・同意」に違反しているとして、フランスのデータ保護機関(CNIL)がグーグルに対して約 62 億円の制裁金を課し、反論する米国と調整しているといわれています。

米国は、一律の規制をせず、個別に規制するという原則ですが、2020 年１月には GDPR に続き、カリフォルニア州が**「消費者プライバシー法」(CCPA)**の施行をめざしています。

（４）SNS「個人関連情報」の取扱いをどうする？

現在の保護法では、SNS でプラットフォーマーが取得可能な「個人関連情報」を規定していません。2020 年に予定される保護法の改正原案(2019.4.25)では次のように提言しています。「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。」としており、**法制化が難しいようです。まず、実態を踏まえ対応する。個人情報保護法だけではカバーできないのではないかと提言しています。**

一方、公取委は、独禁法の「優越的地位の乱用」を防止する観点から、プラットフォーマーと呼ばれる GAFA など IT 大手による個人データの不適切な収集・利用を規制することを検討しており、７月中にも最終案を示し意見を公募します。(2019.7.17 日経朝刊)

指針案では、対象とするデータを**「消費者個人と関係する全ての情報」**として、住所・氏名だけでなく、**サイトの閲覧や購買の履歴・位置情報も含まれる**としています。保護法が「事業の用に供する個人情報」を対象としている事に対して、消費者個人にも適用する方向です。

SNS の個人関連情報の取扱いの基本原則が、論議の只中にある中で、SNS の利用は拡大していますが、SNS の危険な落とし穴も見えてきています。

LINE メッセージの誤送信トラブル、詐欺・なり済ましなどのネット犯罪に巻き込まれる危険、WIFI 通信の傍受などによる情報盗取、スマホ端末の不適切利用、望まない「炎上」、いわゆる「SNS 疲れ」などです。

しかしながら、SNS は「人と人との社会的な繋がりを維持・促進するサービス」として、事業者の顧客拡大、事業詳細の PR など、その活用分野を広げ、利用メリットは今後ますます拡大していくことは間違いと思われます。

「我々の事業に見合った SNS やその『個人関連情報』取扱の枠組み」作りを模索先取りしながら、セキュリティ対策を実務で徹底し、個人の権利利益を保護しつつ、創意工夫による SNS 利活用分野の拡大を目指したいものです。

２．事例に学ぶ：テレワークに伴うリスク対策

事例シリーズの第５弾になります。今回は何かと話題になっている「働き方改革」に関連し、“テレワーク”について情報セキュリティの切り口で検討してみようと思います。

「働き方改革」は、長時間労働の是正、多様で柔軟な働き方の実現、雇用形態にかかわらない公正な待遇の確保などが目的とされています。各社におかれても色々な施策を実施または検討をされていることと推察します。

しかし、就労時間を減らしても業務量が変わらなければ退社後も作業をせざるを得ないことになりますが、これでは工場における「ラインはきれいだが壁際には仕掛かり在庫の山」と代わりがありません。直接的な業務(作業)時間を効率化するか、無用な移動など価値を生まない行動時間を減らすことが本筋です。そこで注目されているのが「RPA」※1や「IoT」※2などですが、併せて自宅や社外での作業(昨今では“テレワーク”が一般的)があります。

※1：Robotic Process Automation：デスクワーク(主に定型作業)をパソコンの中にあるソフトウェア型のロボットが代行・自動処理する概念

※2：Internet of Things：各種の機器と情報通信を行う概念

テレワークを行う中で、以前は「ファイル交換ソフト」が最大の脅威でしたが、今では沈静化しより以上の危険な状態が現出されるようになっています。ここで、改めて過去を振り返り今日的な課題と対策を検討したく思います。

（１）ファイル交換ソフトで何があったのか

2006 年 2 月、防衛庁を皮切りに政府・官公庁での機密情報の漏洩事案が相次ぎ、翌 3 月に当時の安倍官房長官が記者会見で「Winny」(ウィニー。代表的ファイル交換ソフトの名称)の使用を自粛するよう国民に呼びかけました。

「Winny」自体は純粋に楽曲や映像を他人と共有して楽しむことを目的としたものですが、悪用されると情報流出に繋がります。事案は全て、仕事を持ち帰った自宅の PC に当該ソフトがインストールされていたことが原因とされています。

現在では Windows などの OS やウィルス(マルウェア)対策ソフトで、「Winny」などの稼働抑止や通信経路の遮断をするようになっていますので余り問題ではないと考えますが、テレワークを検討する上では大きな教訓です。

（２）テレワーク環境とプライバシー

テレワークを行う PC やモバイル機器(スマホ、ノート／タブレット PC)を許可制にしている会社が多いと思います。会社支給のものでない限り、それらは個人の所有、即ち「BYOD (Bring Your Own Device) 機器」ですから仕事以外のプライベートな情報が多数格納されているでしょう。インストールしているソフトやデータ、設定パラメータにプライベート情報が含まれることから、本人の承諾なしで会社が実機を操作して点検するのは憚られます。本人の承諾を得るにしても“パワハラ”の危険が伴います。

一方、会社は安全にテレワークをしていることを確認する義務がありますので、“自己点検と報告”を求めることが妥当と考えます。情報セキュリティにおける組織的措置に該当し、チェック項目は当然会社が設定します。

技術的措置としては、各種のセキュリティソフトを会社から支給する、サーバとの接続にVPNやリモートデスクトップ環境を用意する、なども必要です。持ち運ぶPCにはファイルの暗号化(例：Windows10 の BitLocker の活用)を課すことも有効で、そのことで個人使用に支障が出るとは考えられませんので、パワハラには該当しないでしょう。

（3）テレワークに備えた社内ルール

トムソンネットがプライバシーマークの支援先各社さんに提供させていただいている規程(安全管理細則)には、以前から標準として「携帯可能なPC、携帯電話、スマートフォン、タブレット端末等(モバイル機器)の利用」の項を設けてあります。(今後、テレワーク全体を念頭に置いてバージョンアップを検討しますが)

会社資産と私有物と共通で、例えば、

・業務で使用するモバイル機器には、ナンバーロック、リモートロック、データ強制消去等の盗難対策を実施する。
・モバイル機器は、通常の動作に支障がない限り基本ソフト(OS)やアプリケーションを最新版にし、セキュリティパッチを自動適用する。
・モバイル機器には、不正又は危険なアプリケーションをインストールしない。
・モバイル機器に個人情報を保管する場合はSDカードに保管せず、秘匿化の措置を講じる。
・モバイル機器の利用時には、安全なワイヤレスネットワークサービス(Wi-Fi)を利用する。

などを盛り込んでいます。最も怖いのは私用の機器から社外秘の情報が盗み出されることですが、当該の機器自体が被害を受けずとも“踏み台”にされて自社や取引先の攻撃(標的型攻撃、ランサムウェア等々)に加担することも想定しなくてはなりません。キーロガー(マルウェアの一種)でID・パスワードが盗まれる、なども想定内です。

社内規程にルールを定めた後、実際に遵守しているかPDCAサイクルを回さないと意味がありません。「誓約書」のみでは不足で、プライバシーマーク事業者では、点検フェーズで内部監査と共に“運用の確認”(自己点検)が要求されています。そのチェック項目に上記のことを参考にされることをお勧めします。

（4）まとめ

この原稿を書いているさ中、「7pay(セブンペイ)」のサービスが撤退になることが発表されました。不正利用のためのようですが、当事者の意識の低さに嘆息しました。

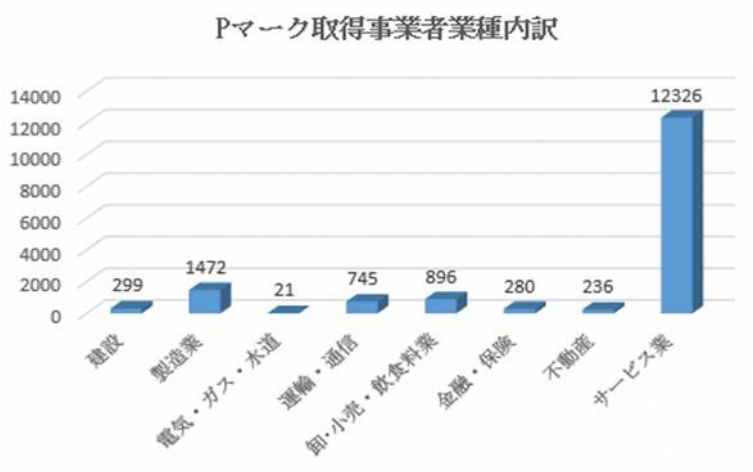
情報セキュリティ維持は、会社の投資と相俟って従業者の皆さんの自覚・関心と注意が欠かせません。内部規程を定めそれを遵守すること、遵守するのが難しいルールであれば理想と現実とで調整を行うこと、そして定期的・適宜にルールの見直しを行うことが鉄則です。テレワークを実践するに際し、プライバシーと会社としての安全確保を両立させる智恵が今後重要性を増してくることは必定です。技術的措置と人的・組織的措置の両輪でテレワークの便宜を享受したいものです。

３．注目される今後の P マーク取得動向

プライバシーマーク（以下 P マーク）制度を統括している一般財団法人日本情報経済社会推進協会（JIPDEC)は、HP 上に P マーク取得事業者の年間推移や業種別内訳を公表しています。

この資料をベースに昨年（2018 年度）のマーク取得動向を追ってみました。

（１）2019 年 3 月末における P マーク取得事業者数は、**16,275 社**でした。前年比では 489 社増加しています。16,275 社の業種別内訳は下図の通りですが、「情報サービス・調査業」が属する**サービス業**が圧倒的に多く、全体の**約 75%**を占めています。



個別業種別ランキング

1	情報サービス･調査業	6,625
2	その他の 事業サービス業	3,253
3	出版･印刷･ 同関連産業	1,257
4	専門サービス業	1,011
5	広告業	549
6	運輸に付帯する サービス業	297
7	道路貨物運送業	259
8	設備工事業	220
9	その他の小売業	181
10	建築材料、鉱物･ 金属材料等卸売業	171
10	保健衛生	171

（２）2018 年度における新規取得動向について

前年度（2018 年）は、P マークの新規取得を目指す事業者にとっては、2018 年 8 月以降新規取得申請は、新 JIS（JIS Q 15001：2017）基準の申請となったため、その動向が注目されました。結果的には、2018 年度の年間の P マーク取得事業者の増加は、約 500 社と新 JIS の影響がなかったかの如く、例年並みの水準で推移しました。

因みに、昨年新規 P マーク取得事業者を増やした業種（ベスト３）は以下です。

No	業種区分	増加事業者数 (年間ｱｯﾌﾟ率)	備考
1	サービス業	398 社（3%）	内、情報サービス・調査業は 222 社増
2	卸・小売・飲食料業	33 社（4%）	
3	製造業	24 社（2%）	

（３）**昨年の状況から現状（2019 年 7 月）の動向を踏まえた注目点**

一見、例年通りの推移に見えますが、以下の点については今後の動向が注目されます。

①金融・保険業は、2018 年度は全業種中、唯一前年比減少を記録しました。その要因は保険業の落込み（前年比 4 社減）ですが、これまでずっと P マーク取得事業者数の増加を続けてきた保険業の変化は、昨年だけの一時的なものかどうか見極めが必要です。

②**現在（2019 年 7 月末）**の P マーク取得事業者数は **16,278 社**です。この数字は 2019 年 3 月末と殆ど変わっていません。直近 4 か月間の全体の増加が 3 社のみというのは、極めて異例な現象です。新 JIS 対応への遅れによる申請の停滞が考えられるところですが、今後、新規取得事業者を増やしていけるのか、注目されます。

４．お知らせ

トムソンネット関連の刊行物をご利用ください。

以下の通り、弊社関連の保険業務に関する書籍のラインナップが充実して参りました。

保険ビジネスの動向や代理店業務の参考として、これらの書籍がみなさまのお役に立つものと確信しております。

各書籍の内容（概要）は、弊社 HP に掲載していますのでご覧ください。

書籍名	出版社
図説損害保険ビジネス（第３版）	金融財政事情研究会
図説生命保険ビジネス	金融財政事情研究会
図説損害保険代理店ビジネスの新潮流	金融財政事情研究会
保険募集制度の歴史的転換	保険教育システム研究所
保険代理店にとっての顧客本位の業務運営	保険教育システム研究所
変わり続ける保険事業	保険教育システム研究所
会社経営トップの賠償責任と保険	保険教育システム研究所

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！

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）

以上