

Pマークニュース

< 2020年新春号 > Vol. 30

株式会社トムソンネット Pマークコンサルティンググループ



2014年の10月に創刊したPマークニュースは、みなさまのご支援により、本号を以って30号を迎えることが出来ました。

創刊以来、みなさまに少しでも「お役に立つ情報の提供を！」との思いから、丁寧な説明を心掛けて参りましたが、そのため記事が次第に長文化し、「ちょっと長くて読むのがシンドイね」とのご意見を頂戴するようになっておりました。

就きましては、30号という区切りを迎え、少しでも「目を通し易い」Pマークニュースとなるべく、若干紙面のスタイルを変更致しました。

具体的には、まず1ページ目に目次（ページ付）と掲載した「記事の概要」を記述しましたので、まず記事概要に目を通して戴き、その中にご興味のある記事をじっくりお読み戴けたら幸いです。

引き続き、Pマークニュースを宜しくお願い申し上げます。

目 次

1. 個人関連情報「クッキー」を巡って・・・・・・・・・・・・・・・・ P2

個人情報の「保護」と「利用」の両面から問題を提起しているのが、Web取引で発生する「クッキー」です。「クッキー」の取扱いは、現在、改正2020個人情報保護法骨子（案）において「個人関連情報」の概念で方向付けが、そして、独禁法ガイドラインで「デジタル・プラットフォームと個人情報等を提供する消費者との取引における優越的地位の濫用に関する独占禁止法上の考え方」で対応が示され、最終的な取り扱いが注目されています。このホットな話題である「クッキー」を採り上げそのポイントを解説します。

2. 事例に学ぶ：「EMOTET」の被害が国内でも拡大・・・・・・・・ P4

「EMOTET」（エモテット）は、感染したパソコンに保存されたメールアドレスや本文を盗み取り、その情報から新たな「なりすましメール」を作り出して自己拡散するウイルスです。実在の人物や組織になりすましたメールに添付されてくるため、うっかりファイルを開いて感染したとみられる被害が後を絶ちません。これから卒業・入学・就職等の時節を反映して、出現する可能性が高まると言われています。記事ではエモテットの感染方法や予防方法を説明して、注意を呼び掛けています。

3. Pマークを取り巻く昨今の状況変化について・・・・・・・・ P6

Pマーク付与事業者数は、この10数年ずっと右肩上がり年間約500社前後の増加を続けてきました。ところが昨年、突然、付与事業者の伸びが大幅にダウンしました。この背景には、JIS Q 15001:2017（新JIS）の存在があるようです。

また、直近の業種別のPマーク動向で目立ったのが、「金融・保険業」の落ち込みです。中でも保険代理店業は顕著な減少傾向にあり、その状況を示しました。一方、今後の増加に繋がることが期待される新たな動きもあり、紹介しています。

4. お知らせ（トピックス）・・・・・・・・・・・・・・・・ P8

以上

1. 個人関連情報「クッキー」を巡って

－ 2020 改正個人情報法・独禁法ガイドラインの対応 －

全世界で 11 兆円と言われるインターネット広告ビジネスでは、ネット利用者の閲覧履歴データ「クッキー」が取得され、広告配信に利用されています。なかでもターゲティング広告は、利用者にとって興味関心のある広告に接する機会が増える利点があります。

一方、知らないうちに企業間で拡散し、趣味や行動パターンの分析にも使われています。

「リクナビ」が就活者の内定辞退予測を企業に販売した問題でも利用されました。「クッキー」をめぐる利活用の促進と個人情報の保護の両立を目指して、2020 改正個人情報保護法の骨子案(2019.11.29)や独禁法ガイドライン(2019.12.17)が公表されました。個人関連情報「クッキー」を巡る動向を追い、保険ビジネスでの活用の方向を探ってみました。

(1) 「クッキー」(Cookie)をめぐる課題

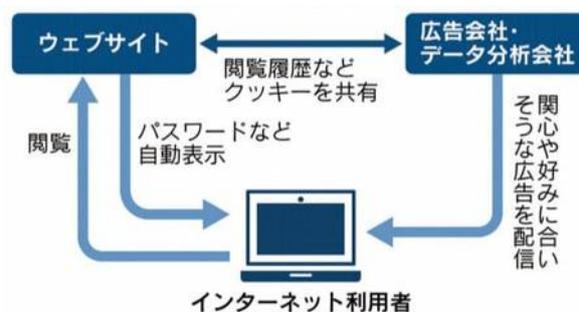
これから採り上げる「クッキー」は新春号ですが、お菓子の「クッキー」では勿論ありません。「クッキー」とは、「利用者の Web ブラウザと Web サイトを運営するサーバ間で特定の情報(閲覧したページやパスワードなど)をやり取りする情報をファイルにして記憶したもの」です。

「クッキー」が利用者のコンピュータに保存されることにより、次回以降に「クッキー」発行元の Web サイトを訪れた際に、前回の続きのページを表示できます。この「クッキー」を Web サイトと広告企業・データ分析企業が共有して、複数のサイトの情報を結び付ければ「関心や好みに合いそうな広告の配信」も可能になります。例えば、京都の観光地に関するサイトをよく検索していると次第に京都のホテル・観光地に関する広告が増えることがあります。これはネット広告企業が「クッキー」を分析し、「この人は京都観光に興味がある」と推定したためです。

このように、利用者に関する情報を活用した**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ィー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恐れなどです。**個人情報保護の課題**です。

また、「クッキー」は「ターゲティング広告」(狙う広告)を配信するために使われても来ました。「ターゲティング広告」は、現在約 11 兆円の巨大産業となり、この 5 年で 5 倍に増え、ネット広告の約 7 割を占めるといわれています。(日経 2020.1.8) この Web サイト運営先である Google、フェイスブックなど巨大 IT 企業への独占的な動きに対する規制がはじまっています。**巨大 IT への規制の課題**です。



(2) 2020 個人情報保護法骨子(案)(2019.11.29)はどう対応するか?

「クッキー」は、個人情報保護法上の「個人情報」ではありません。クッキー等の識別子情報や位置情報、閲覧履歴、購買履歴といったログ情報等の個人に関する情報で、個人を特定することができないもののプライバシー上の懸念が生じ得る情報を「インフォマティブデータ」とし、個人情報保護法における「個人情報」と「インフォマティブデータ」から「統計情報」を除いたものを2020 個人情報保護法骨子(案)では、「**個人関連情報**」としています。(日本インタラクティブ広告協会 (J I A A) 「プライバシーポリシーガイドライン」)

従って、「クッキー」を「個人情報」の規制ではなく、わかりにくい表現ですが、2020 個人情報保護法骨子(案)では、「提供先において個人データとなる場合の規律の明確化」として、「個人に関する情報の活用手法が多様化する中であって、個人情報の保護と適正かつ効果的な活用のバランスを維持する観点から、提供元では個人データに該当しないものの、提供先において個人データになることが明らかな情報について、個人データの第三者提供を制限する規律を適用する。」としています。EU の GDPR が「クッキー」を「個人情報」として扱い、取得、第三者提供のルールを適用する事と異なります。「クッキー」を「**提供元では個人データに該当しないものの、提供先において個人データになることが明らかな情報**」とし、「**個人を特定する企業に渡す場合**」の規制が必要で、その際はその旨の本人からの同意が必要と改正されることになりそうです。利活用の拡大を主張する経済界にも配慮したきめ細かな対応です。

(3) 独禁法ガイドライン(2019.12.17)ではどう対応するか?

公正取引委員会は、「デジタル・プラットフォーマーと個人情報等を提供する消費者との取引における優越的地位の濫用に関する独占禁止法上の考え方」を公表し、2020 改正個人情報保護法と同様に「提供元では個人データに該当しないものの、提供先において個人データになることが明らかな情報について、利用者に利用目的を示した上で取得しなければならない。」とし、利用者に不利益を与えた場合やあらかじめ示した利用目的を超えた範囲で取得した場合などは、独占禁止法違反にあたるとしています。また、違反が認定されれば、行政処分の対象となるとしています。「クッキー」の取得や利用についても**独禁法の規制を設けたこと**になります。

(4) 今後「クッキー」の利用をどうするか?

「ターゲティング広告」(狙う広告)に「クッキー」を使わず、代替技術を模索し、個人情報の保護を優先する動きも報道されています。(日経 2020.1.8) また、グーグルが同社「クローム」でのネット閲覧履歴の外部提供を2022年までに取りやめると公表しています。**個人データ乱用への懸念が高まり、個人情報保護の機運**を大きく後押ししそうです。

保険業界での「クッキー」利用のニュースは多くはありませんが、「『リクナビ』の就活者の内定辞退予測販売事件」で、その利用会社として行政指導された会社37社に、アフラック生命保険、太陽生命保険があり、データを扱う社内体制の不備が指摘されました。

今後、Web サイトとの「クッキー」の共有条件が厳格化されれば、**自動車運転行動履歴、病歴など保険引き受けに関する情報データの取得・利用**は、法規制をよく理解し、自力で取り組むことがますます必要となるでしょう。きめ細かな顧客情報の取得が企業の優劣を決めることとなります。「クッキー」に対する法規制の理解を深め、個人情報保護を意識し、「クッキー」の有効な利活用を自社でどう展開するかが、ポイントとなってきます。

2. 事例に学ぶ：「EMOTET」の被害が国内でも拡大

事例シリーズの第7弾になります。今回は昨年(2019年)国内で被害が急増しているマルウェア(ウイルスを含む不正ソフト)「EMOTET」について取り上げます。

インターネットを介して発生する侵入の被害や妨害等の情報を統括管理する政府機関・JPCERT コーディネーションセンター (JPCERT/CC) は2019年12月27日、「マルウェア EMOTET の感染に関する注意喚起」を発表しました。続いて翌日に記者会見で菅義偉官房長官が感染被害の発生と行政機関や東京オリンピック関連の事業者に注意喚起を行っていることを明らかにするなど、大きな脅威となりつつあります。

「EMOTET」は「エモット」と読み、実は6年前に出現したもののようですが、主に米国で流行しており日本国内では被害が表面化していませんでした。後述のように主な感染源がメールで、件名や本文が英語だったためと考えられますが、それらが日本語のものが1年程前から出回るようになり、9月頃から急激に被害が広がっています。

(1) EMOTET の恐ろしさ

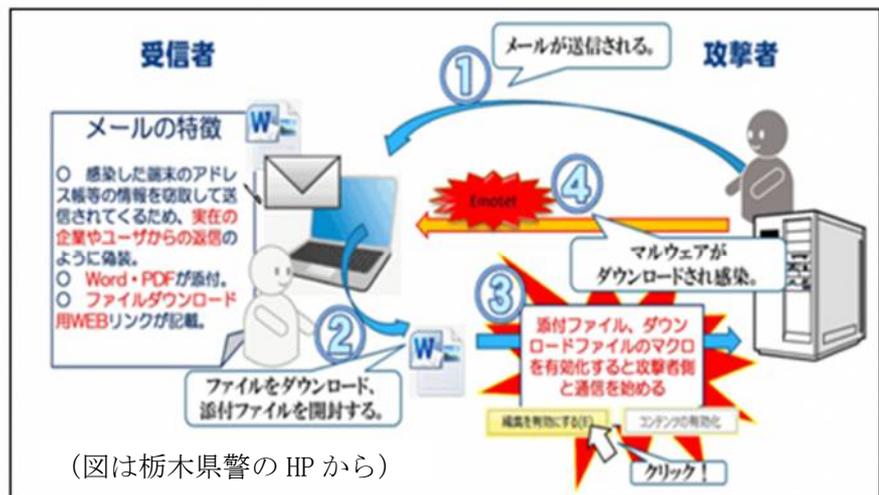
EMOTEの手口は、攻撃先が関心を持ちそうな内容にしたり、窃取したメールに対する返信の形でメール送信します。従って、一見すると不審メールに見えないため被害に遭う可能性が高まります。

添付ファイルや本文中のURLによっ

て「バックドア」が仕掛けられ、そのPCが何をされるか分かったものではありません。

例えば、標的型攻撃の踏み台にされたり、PCを人質にするランサムウェア、或いはオンラインバンキングのID、パスワード、暗証番号を盗むバンキングトロジャンを仕込まれたり、会社の他のPCにも伝播します。

「バックドア」は「裏口」または「勝手口」のことで、捕り物小説に登場する「引き込み」のような役目を果たし、外部から当該のPCを操作できる環境を整えます。



(図は栃木県警のHPから)

(2) どのように感染するのか

感染ルートは主にメールです。件名であれば、以下のようなものです。

業務・私的義務型	好奇心喚起型	時節反映型
あなたの請求書 サービス請求書 延滞請求書 期限切れ請求書 支払請求書 支払明細通知書 請求書	コメント データ ドキュメント メッセージ リマインダー 一覧 新バージョン	賞与 2019冬・業績賞与支給 クリスマス 謹賀新年 明けましておめでとう 被災地の子どもたち コロナウイルス

特に注意したいのは「時節反映型」です。これから「卒業」、「入学」、「就職」、「昇進」、等の出現が予想されます。

本文でも次のように極く普通の日本語が使われています。左は添付ファイル型で、右が不正 URL を開かせる型です。

お世話になります。	いつも大変お世話になっております。
11 月分の請求書を添付致します。	◆振込データ情報 口座 : ○○○○銀行
色々とお手数をおかけしますが、宜しくお願 い致します。	明細は以下にあります。 http://.....

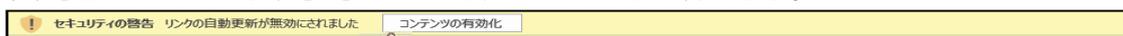
(3) 予防方法は

予防法の大原則は OS やマルウェア(ウイルス)対策ソフト、アプリケーションソフトのセキュリティパッチを適宜に適用することですが、他に人間系対策として以下のものがあります。

①添付ファイル型の予防

端的に言えば、件名も本文も真つ当な日本語文となっていますので添付ファイルを開く所までは行く可能性が高いと考えるべきです。

問題はその後で、「マクロを働かせない」ようにすることが肝要です。添付ファイルを開く(ダブルクリックする)と次のメッセージが黄色く表示されます。そこで[コンテンツの有効化]をクリックせず、[×]で Word を閉じれば無事に済みます。



②不正 URL 型の予防

本文中にある URL (http://.....) をチェックしましょう。とは言っても実際に開くのは危険ですから、URL チェックサイトに検査を依頼すれば結果を返してもらえます。URL チェックサイトには「https://www.aguse.jp/」、「http://check.gred.jp/」等があります。不正サイトはすぐに閉鎖しますので、「コンテンツが取得できない」、等の表示があるかもしれません。

(4) まとめ

メールがサイバー被害の源になることは今まで散々言われていたことです。被害に遭わないためには添付ファイルは安易に開かない、正式な会社名をドメインにしていない URL にアクセスしない等々、今までも沢山の予防措置が挙げられています。

ただ、EMOTET については件名も本文も真つ当な日本語で、添付ファイルの名前も本文といかにも関連がありそうなものになっていることから、これまでの対策では通用しない場合があります。少しでも怪しいと思えるメールが届いた際には、間髪を入れず管理者に報告し相談するようにしましょう。

余談になりますが、ファイルの暗号化に「zip では弱い」と盛んに喧伝されるようになっていきます。現に定番ソフトの「Lhaplus」にはメニューにパスワードを暴くタブが堂々と表示されます。引き続き zip をお使いの場合は、「英数字の混合」と「8 桁(できれば 12 桁)以上」にして暗号解読の時間を長引かせることを心掛け、本当に重要なファイルには他のソフト(例えば「アタッシュケース」)の使用を考慮いただきたく思います。

zip では設定した文字数が総当たりの対象になりますが、「アタッシュケース」では設定した文字に乱数を加えて 32 文字(標準)に増やすことで、事実上総当たりが非現実的な状態にします。

3. Pマークを取り巻く昨今の状況変化について

(1) JIS Q 15001 : 2017 (以下新 JIS) 適用に伴って生じている事象

新 JIS は 2017 年 12 月に公表され、以下の新 JIS 適用スケジュールに沿って運用されております。
(以下の新 JIS 適用スケジュールおよび P マーク付与事業者数等は JIPDEC 公表資料より)



現時点(2020/2)では、Pマークの新規審査は全て新 JIS が基準となっています。また、継続更新審査は 2020 年 7 月 31 日までは、旧基準と新 JIS が並行する移行期間となっています。今回の JIS 改訂は、約 10 年振りに実施された個人情報保護法改正に伴うもので、JIS Q 15001 にとっても 11 年振りの改訂となりました。このため、P マークの取得動向に与える影響が注目されておりましたが、状況は以下の通りとなっています。

時期	2018/09	2019/03	2019/09	2020/1 (*)	備考
事業者数	15,969	16,275	16,346	16,413	(*) 2020 年 1/末
期間増加	181	306	71	67	現在

上表の通り、まだ移行期間中であり、断定的な判断は出来ませんが、2018 年 4 月以降の P マークの取得や継続を巡る動きには、新 JIS への移行の影響と思われるものが示されています。具体的には、

- ①2019 年 9 月および 2020 年 1 月の P マーク付与事業者の増加数です。2019 年 4 月以降の増加が、従来に比べて大幅にダウンしています。減少要因は、新規取得の減少と継続更新の取止め増加が重なったものと思われます。
- ②新規取得が減少した要因としては、P マークの新規取得審査が 2018 年 8 月以降は新 JIS 基準となったため、事業者が用意する審査に不可欠な「個人情報保護マネジメントシステム(PMS)」の規程は、新 JIS 対応が必須となりました。この規程対応が P マークを取得しようとする事業者やそれを支援するコンサル会社においてスムーズに進まなかったことが一因と考えられます。
- ③また、P マークの継続更新審査においても、上記の②の規定対応が高いハードルとなって、更新の継続を断念する事業者が多く出て、P マーク付与事業者の減少に繋がりました。
- ④なお、上表において 2018 年 10 月から 2019 年 3 月の期間は、半期で 306 件と例年以上の伸びを記録しています。この時期については、新 JIS 基準の審査移行を前に、従来の PMS 規程による旧 JIS 基準による駆け込み的な新規取得で増えたことが窺われます。

⑤今後の見通しとしては、個人情報に対する社会的な関心は益々高まっており、P マーク自体の有用性は高まっても低下することはないものと思料されます。このため、昨年のP マークの新規取得・更新継続の落ち込みは一時的なもので、今後は新 JIS 規程の定着化とともに、徐々に従前の増加水準に戻って行くものと思われまます。

(2) 保険代理店の気になるP マーク動向について

下表は、保険代理店の直近5年間のP マーク新たに取得した保険代理店とP マークの更新を取止めた保険代理店について弊社で集計したものです。

年度	2015年	2016年	2017年	2018年	2019年
新規取得代理店数	16	15	11	7	3
更新見合せ代理店数	5	4	2	13	7
年度増減数	11	11	9	-6	-4
P マーク取得代理店数	114	125	134	128	124

2018年から急に「新規＝伸び悩み」、「更新取止め＝増加」が顕著になったことが分かります。そこで他業種の最近1年半の動向と比較したのが下表です。「金融・保険業」は表に示した業種別の推移表の中で、唯一P マーク付与事業者を減らした業種です。また、金融・保険業が大きく落ち込んだ主たる要因は、上表からも「保険代理店業」の急激な減少と言えます。

業種区分	時期	2018/3 (A)	2018/9	2019/3	2019/9 (B)	(B) - (A) 増減
建設業		291	298	299	304	13
製造業		1,448	1,461	1,472	1,458	10
電気・ガス・熱供給・水道業		20	21	21	22	2
運輸・通信業		731	731	745	750	19
卸売・小売業、飲食店		863	877	896	897	34
金融・保険業		284	284	280	276	-8
不動産業		223	230	236	243	20
サービス業		11,928	12,072	12,326	12,396	468
合計		15,788	15,969	16,275	16,346	13

保険代理店業は、当局および保険会社から厳正な個人情報管理が求められています。このため、現在のようなP マーク付与事業者の減少は、理解し難い事象と言えますが、更新を取止めた理由として「担当者が退職して後任がいなくなった/P マークの保守・運用を更新できる水準で維持できなかった」等々、個々の保険代理店の事情が聞こえます。

その一方では、近時、アフラックや東京海上日動あんしん生命の直資代理店がP マークを取得したことや、保険代理店の意欲的経営を進める若手経営者が、コーポレートガバナンス強化の観点からP マークを取得するといった動きも出ており、再び増勢に転ずる時期は近いものと期待されます。

4. お知らせ（トピックス）

(1) 情報処理推進機構（IPA）が「情報セキュリティ 10 大脅威 2020」を 2020.1.29 に公表しました。組織（企業）における脅威のトップは、「標的型攻撃による機密情報の窃取」になっています。10 大脅威とそのランキングは下表の通りです。

■「情報セキュリティ10大脅威 2020」

NEW : 初めてランクインした脅威

昨年 順位	個人	順位	組織	昨年 順位
NEW	スマホ決済の不正利用	1位	標的型攻撃による機密情報の窃取	1位
2位	フィッシングによる個人情報の詐取	2位	内部不正による情報漏えい	5位
1位	クレジットカード情報の不正利用	3位	ビジネスメール詐欺による金銭被害	2位
7位	インターネットバンキングの不正利用	4位	サプライチェーンの弱点を悪用した攻撃	4位
4位	メールやSMS等を使った脅迫・詐欺の手口による金銭要求	5位	ランサムウェアによる被害	3位
3位	不正アプリによるスマートフォン利用者への被害	6位	予期せぬIT基盤の障害に伴う業務停止	16位
5位	ネット上の誹謗・中傷・デマ	7位	不注意による情報漏えい（規則は遵守）	10位
8位	インターネット上のサービスへの不正ログイン	8位	インターネット上のサービスからの個人情報窃取	7位
6位	偽警告によるインターネット詐欺	9位	IoT機器の不正利用	8位
12位	インターネット上のサービスからの個人情報窃取	10位	サービス妨害攻撃によるサービスの停止	6位

(2) 総務省の発表（2020.1.20）によれば、個人カード（マイナンバーカード）の交付率が漸く 15% に達しました。

区分	人口（2020.1.1 現在）	交付枚数（2020.1.20 現在）	交付率
全国集計	127,443,563 人	19,101,271 枚	15.0%

以上

Pマークをはじめとして各種ご相談は下記で承っています。お気軽にどうぞ！

連絡先 株式会社トムソンネット (<http://www.tmsn.net/>)

〒101-0062 東京都千代田区神田駿河台 4-6 御茶ノ水ソラシティ 1 3 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)