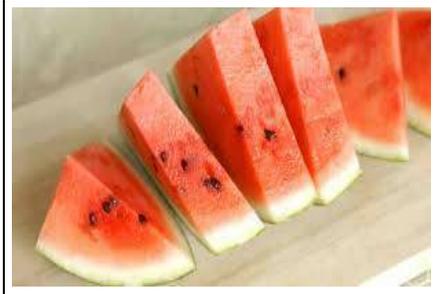


Pマークニュース

<2021年盛夏号> Vol. 36

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



目次と記事概要

1. 事業者に加えて課せられる規制 — 改正法のポイント — P2

2020改正個人情報保護法の施行が2022年4月1日となりました。法の「ガイドライン」が示され、パブコメを経て、今秋には正式に公表されることとなっています。今回の記事では、主な改正点のうち、「不適正利用の禁止」「公表事項の充実」「利用停止請求権の拡大」を採り上げ、そのポイントを概観しました。「不適正利用の禁止」等いずれも、実務的にも影響が出てくる箇所であり、留意点等についても分かり易く説明しています。

2. 事例に学ぶ：情報セキュリティの脅威が新たなステージに P6

毎年のように進化する情報セキュリティの脅威（サイバー攻撃）は、コロナ禍にあっても一向に衰えず、昨年辺りからワンステップ上がり、新たなステージに入っていると言われています。「新たなステージ」とは具体的には、「攻撃のパターンが標的型攻撃とランサムウェアの融合型になり金銭被害が二重に嵩む事例が増えている」ことです。こうしたサイバー攻撃は、とかく自社には関係のない事案と考え勝ちですが、決して別世界の話ではありません。今回の事例に学ぶでは、サイバー攻撃の被害を回避するための「対策」を中心に纏めました。じっくりとお読みください。

3. 保険代理店のPマーク新規取得に復調の兆し P9

ここ2、3年、保険代理店のPマーク新規取得の不振が、目立っておりまして。また、新規取得の不振にとどまらず、Pマークの更新継続を見合わせる保険代理店が相次ぎ、「保険代理店にPマークはもう必要ないのか？」と思わせるほどでした。ところが、2021年になってこの様相に変化が生まれてきました。具体的には、既に8月までに7社の保険代理店が新たにPマークを取得し、さらに現在新規取得に向けて準備中の保険代理店も数社ある模様です。今年は久しぶりに、「新規取得年間10社超え」が期待されます。そこで2021年に新たにPマーク取得した7社を調べ、増加要因等を探ってみました。

4. お知らせ（トピックス） P11

以上

1. 事業者を追加して課せられる規制 — 改正法のポイント —

2020 改正個人情報保護法の施行が 2022 年 4 月 1 日となりました(政令第 55 号)。

法の「ガイドライン」が示され、パブコメ(2021.6.18 締切)を経て、2021.秋には正式公表されることとなっています。今回は、主な改正点のうち、「不適正利用の禁止」「公表事項の充実」「利用停止請求権の拡大」について、そのポイントを概観します。

(2020 改正個人情報保護法については、本誌の 2020 陽春号以降順次概説しています。詳細は末尾をご参照ください)

(1) 不適正利用の禁止

現行法の規定に照らして違法ではないとしても、違法又は不当な行為を助長し、又は誘発するおそれのある方法により個人情報を利用するなど、潜在的に個人の権利利益の侵害につながるものが懸念される個人情報の利用の形態がみられます。

本法の目的である個人の権利利益の保護に照らして、看過できないような方法で個人情報が利用されている事例が、一部にみられることから、「不適正な利用の禁止」として、法第 16 条の 2 を新設し、「個人情報取扱事業者は、違法又は不当な行為を助長し、又は誘発するおそれがある方法により個人情報を利用してはならない。」としています。

その明確化のため、ガイドラインでは下記の具体例を挙げています。見過ごされている「提供」の取扱いの厳格化を求めており、留意が必要です。(該当する事例)

- 個人情報を提供した場合、提供先において法第 23 条第 1 項(提供の原則 本人同意)に違反する第三者提供がなされること。
- 個人情報を提供した場合、提供先において法第 23 条第 1 項(提供の原則 本人同意)に違反する第三者提供がなされることを予見できるにもかかわらず、当該提供先に対して、個人情報を提供すること。
- 採用選考を通じて個人情報を取得した事業者が、性別、国籍等の特定の属性のみにより、正当な理由なく、本人に対する違法な差別的取扱いを行うために、個人情報を利用すること。
- 広告配信を行っている事業者が、第三者から広告配信依頼を受けた商品が違法薬物等の違法な商品であることが予見できるにもかかわらず、当該商品の広告配信のために、自社で取得した個人情報を利用すること。
- 違法な行為を営むことが疑われる者(例：貸金業登録を行っていない貸金業者)からの突然の接触による本人の平穏な生活を送る権利の侵害等、当該違反事業者の違法な行為を助長するおそれが想定されるにもかかわらず、当該違反事業者に当該本人の個人情報を提供すること。
- 裁判所による公告等により散在的に公開されている個人情報(例：官報に掲載される破産者情報)を、当該個人情報に係る本人に対する違法な差別が、不特定多数の者に

よって誘発されるおそれがあることが予見できるにもかかわらず、それを集約してデータベース化し、インターネット上で公開すること。

- 暴力団員により行われる暴力的要求行為等の不当な行為や総会屋による不当な要求を助長し、又は誘発するおそれが予見できるにもかかわらず、事業者間で共有している暴力団員等に該当する人物を本人とする個人情報や、不当要求による被害を防止するために必要な業務を行う各事業者の責任者の名簿等を、みだりに開示し、又は暴力団等に対しその存在を明らかにすること。

(2) 公表事項の充実

消費者自らの情報の取扱いに対する関心や、関与への期待が高まる中、またAI・ビッグデータ時代を迎え、個人情報の活用が一層多岐に亘るところから、事業者が個人情報を取り扱う際に、本人の権利利益との関係で説明責任を果たしつつ、本人の予測可能な範囲内で適正な利用がなされるよう、環境を整備していくことが重要との判断から、下記の公表事項の追加を規定しました。

①安全管理のために講じた措置の公表。

事業者に求められる安全管理措置は様々であるため、法第20条の安全管理措置規定は、措置の具体的な内容を一律に規定していません。同様に、その公表についても、内容を一律に規定することは望ましくないと考えられます。

(公表すべき事項として示された事項)

- ・内部体制の整備(取得、利用、廃棄といった段階ごとに、取扱方法や担当者及びその任務等について規定を策定し、定期的に見直しを実施している旨等)
- ・組織体制の整備(責任者など設置している旨及びその役職・任務等、漏えい等を把握した場合の報告連絡体制等)
- ・定期点検・監査(定期的な自己点検、他部署監査、外部主体監査の実施等)
- ・従業員の教育(定期的研修を実施している旨、秘密保持に関する事項を就業規則等に盛り込み周知している旨等)
- ・不正アクセス等の防止(外部からの不正アクセスから保護する仕組みを導入している旨等)
- ・外的環境の把握(外国で個人データを取り扱っている場合の外国の個人情報保護制度等)

(支障を及ぼすおそれがあるものとして示された事項)

- ・個人データが記録された機器等の廃棄方法、盗難防止のための管理方法
- ・個人データ管理区域の入退室管理方法
- ・アクセス制御の範囲、アクセス者の認証手法等
- ・不正アクセス防止措置の内容等

②利用目的の具体的な公表（本人が予測できる程度に）

利用目的の規定に関し、本人が合理的に予測等できないような個人データの処理（ex.所謂「プロファイリング」）が行われる場合、本人が予測できる程度に利用目的を特定しなければならない旨の明確化を規定しています。

（具体的な利用目的の表示の例示）

- ・ 閲覧履歴や購買履歴等の情報を分析することによって、本人の趣向等に応じた広告を配信するケース（「○」…適切／「×」…不十分）
 - …取得した閲覧履歴や購買履歴等の情報を分析して、趣向に応じた新商品・サービスに関する広告のために利用いたします。
 - ×…広告配信のために利用いたします。
- ・ 履歴書や面接で得た情報のみならず、（本人が分析されることを想定していない）行動履歴等の情報を分析し、人事採用に活用するケース
 - …履歴書や面接で得た情報に加え、行動履歴等の情報を分析して、当該分析結果を採否の検討・決定のために利用いたします。
 - ×…取得した情報を採否の検討・決定のために利用いたします。
- ・ 行動履歴等の情報を分析の上、結果をスコア化した上で、当該スコア（自体を提供することを本人に通知等することなく）を第三者へ提供するケース
 - …取得した行動履歴等の情報を分析し、結果をスコア化した上で、当該スコアを第三者へ提供いたします。
 - ×…取得した情報を第三者へ提供いたします。

③外国の制度等を把握した上での安全管理措置を講ずべき旨の明確化

詳細 省略

（3）利用停止請求権の拡大

一部の法違反の場合に加えて、本人の権利又は正当な利益が害されるおそれがある場合にも拡充することを規定しました。下記事項です。

- ①第22条の2第1項本文に規定する事態(重大な漏えい等(要配慮個人情報、財産的被害、不正の目的、千人超)が生じた場合
- ②利用する必要がなくなった場合
 - ・ダイレクトメールを送付するために保有していた情報について、本人からの求めを受け等して、ダイレクトメールの送付を停止した後、本人が消去を請求した場合
 - ・キャンペーンの懸賞品送付のために保有していた当該キャンペーンの応募者の情報について、懸賞品の発送が終わり、不着対応等のための合理的な期間が経過した後に、応募

者が利用停止等を請求した場合

- ・採用応募者のうち、採用に至らなかった応募者の情報について、再応募への対応等のための合理的な期間が経過した後に、採用応募者が利用停止等を請求した場合

③本人の権利又は正当な利益が害されるおそれがある場合

- ・ダイレクトメールの送付を受けた本人が、送付の停止を求める意思を表示したにもかかわらず、個人情報取扱事業者がダイレクトメールを繰り返し送付していることから、本人が利用停止等を請求する場合
- ・個人情報取扱事業者が、法第 23 条第 1 項に違反して第三者提供を行っており、本人を識別する保有個人データについても本人の同意なく提供されるおそれがあることから、本人が利用停止等を請求する場合
- ・個人情報取扱事業者が、退職した社員の情報を現在も自社の社員であるようにホームページ等に掲載し、これによって本人に不利益が生じていることから、本人が利用停止等を請求する場合。

【2020 改正個人情報保護法関連の解説記事】 下記の P マークニュースを参照ください。

- ・ 2020 改正個人情報保護法の概要 2020 盛夏号 32 号
- ・ 漏洩など報告と本人通知義務、法定刑の引き上げ 2020 爽秋号 33 号
- ・ 仮名加工／個人関連情報 2020 個人情報保護法が改正されました 2021 陽春号 35 号

2. 事例に学ぶ：情報セキュリティの脅威が新たなステージに

事例シリーズの第 12 弾になります。本稿では、毎年のように進化している情報セキュリティの脅威(サイバー攻撃)が、昨年辺りからワンステップ上がり新たなステージに入っているように感じますので、改めて対策を考えてみたいと思います。とはいえ、高額 of 投資をお勧めする訳ではなく、人間系で検知や予防ができることは人間系でと考えています。

ついこの春(5月)、米国で大手燃料供給会社の Colonial Pipeline 社(以下コロニアル)を狙ったランサムウェア攻撃が話題になりました。この事案は、「Darkside」(ダークサイド。以下 DS)と名乗るサイバー犯罪者グループの仕業であるとされています。DS は「インターネットの闇」として著名でしたが、この件により更に注目を浴びることになりました。

国内でも、あるプライバシーマーク事業者でフォルダ共有システム「Samba」の脆弱性を突かれ Samba サーバ内のデータを DS に吸い上げられた事故が発生しています。幸い悪用された形跡はありませんが、どこまで拡散しているか戦々恐々です。



(1) 新たなステージとは何か

「新たなステージ」を端的に言えば、攻撃のパターンが標的型攻撃とランサムウェアの融合型になり金銭被害が二重に嵩んでいることです。

今までのランサムウェア攻撃は相手構わずマルウェア(ウィルスを含む不正ソフト全般)をインストールさせて PC を暗号化で使えなくし、お金を払えば暗号を解くキーを教えると言う手口でした。一方、標的型攻撃は定めた攻撃先の PC にマルウェアを送り込み、それを介して情報を盗み出すと言うもので必ずしも金銭との関わりはありませんでした。ところが、コロニアルの場合は、資金が潤沢と目されるエネルギー業界に狙いを絞った(標的型です)ランサムウェア攻撃であることが明らかになっており、端末のロック解除と引き換えに「身代金」を要求するだけでなく、窃取した情報の代金も要求するという「情報暴露」の「二重脅迫」の手口を駆使しています。実際に 4.8 億ドルを収奪したようです。

ではどうして攻撃先の PC に入り込めたのか・・・。コロニアルの事案が発覚する直前に、別の集団がパイプラインのメンテナンスを行っている会社からコロニアルを含む取引先の

情報を盗み出して自らのダークウェブサイトに公開しました。それを手に入れた攻撃者がコロニアルを標的にしてランサムウェアを仕込んだことは十分に考えられます。

コロニアルの事案で攻撃の「入口」が、メールかその他の方法かは公表されていませんが、各社の Web サイトにある問い合わせフォームなどに不正サイトに誘導する文章を入力する手口も警告されています。添付ファイルを安易に開かないなど、危険メールの対策が大分浸透してきた現在、新たに別なルートが露呈したことになります。問合せや社員募集などフォームの入力データの添付資料に「Emotet」などのマルウェアが仕掛けられることも予想されます。

(2) 新たな対策が必要か

結論から言えば、旧来からの防御策を緻密に実施することで予防できると考えます。

二重脅迫であっても原因は一つで、多くの場合入口はメールや Web サイトでの不用意なクリックによるものです。

IPA(情報処理推進機構)は古くから以下の 4 つのポイントを公表し注意を喚起しています。
(<https://www.ipa.go.jp/security/personal/base/mail/point1.html>)

なかに「添付ファイルに要注意」、「メール本文を HTML 表示しない」などが含まれており、今現在においても有効ですが、近年のサイバー攻撃ではメールに添付ファイルがなく、文面も違和感のない日本語になっています。メール自体は何の害を及ぼすものではなく、問題は本文に含まれる URL が不正サイトであることです。

技術的措置として、隔離された環境で URL や添付ファイルを検査(疑似実行)させる「サンドボックス」を導入し防御を図るのは勿論有効ですが、予算措置が必要です。出来る限り従業員の「眼」で防御したいものです。

(3) 新しい技術的対策は何か

近年、マルウェアの侵入を防御する「入口対策」と共に注目されているのは侵入を前提に被害を極小化しようとする「出口対策」です。

標的型攻撃は、メールなどを使って PC にバックドア(裏口)ソフトをインストールさせ、リモートデスクトップのように外部から操作し当該の PC や LAN 上に存在するサーバや他の PC 内にある情報を探り(調査段階)、対象を定めて攻撃を開始する(実行段階)フローで行われます。この調査段階で「C&C サーバ」と呼ばれるサーバと通信しシステムファイルに異常なアクセスを行うことから、Windows Defender など各種のマルウェア対策ソフトは検知を図り、PC の中で動作ログを緻密に取るようにもしています。

また、メール本文中に怪しい URL があった場合、大半はマルウェア対策ソフトで迷惑メールに仕分けされていることでしょう。

とは言え、日々進化するマルウェアに対し技術的対策で間髪を入れず完璧に防御するのは無理があり、人間系(人的対策・措置)に依存する点は皆無になりません。

(4) 人的措置で技術的対策を補完するには

ここで言う「人的対策」とは、従業員の皆さんの注意力や観察眼を研ぎ澄ますこと、即ち「見極め」になります。

見極めのポイントは「ドメイン」です。ドメインは、サーバに外部用に振られた名前で、

メールアドレスの場合 ●●●●@aaa.bbb.ccc

Web サイト (URL) の場合 http://○○○.aaa.bbb.ccc

http://○○○.aaa.bbb.ccc /△△△.△△.△△/□□

の「aaa.bbb.ccc」で表される部分で、全世界で重複することがないように管理する機関があります。一般に、aaa に会社名、bbb に業種、ccc に国名を割り当てますが、「.com」のように ccc がなく bbb でも業種を表現していないものもあります。●●●●は氏名が多く、○○○は「www」が一般的です。

先だって「Amazon.co.jp 重要情報の更新:お支払い方法変更のお願い」の件名でメールがきました。本文中に「https://dns-amazon.lting.top」をクリックするように促す文が入っていました。このドメインは「dns-amazon.lting.top」です。正規の通知であれば amazon.co.jp か amazon.com でしょうから怪しいと分かります。ただし、この URL (文字列) を見るができるのは、前述の IPA の推奨通り受信メールをテキスト形式で表示するように設定している場合に限りです。(HTML 表示の場合はその URL のコンテンツが表示されます)

メールについては「ヘッダー」情報をチェックしましょう。

Outlook では受信フォルダなどにある当該のメールをクリックし「メッセージオプション」でヘッダーが見ることができます。ヘッダーのなかで注目する項目は「Return-Path:」と「Reply-to:」で、その後にあるアドレスのドメインを見ると正規の会社から発信されたものかどうかの判別ができます。上記のメールの Return-Path は「kefu@ssjiy kz.cn」でした。

(4) 終わりに

サイバー攻撃への備えとして、技術的措置は Windows の頻繁なアップデートに見られるよう日進月歩です。マルウェア対策ソフトも毎日のようにパターンファイルの更新があります。

しかし、自社の Web サイトのフォームから入力され管理者にメールとして送信されたメッセージは、Web サーバが設定したアドレスが入るため「Return-Path」や「ドメイン」のチェックはすり抜けます。メッセージ本文に含まれた URL と履歴書など添付ファイルへの注意は基本中の基本であり、益々重要性を増しています。キーは「ドメイン」にあると考えます。

攻撃メールへの訓練サービスを行っている会社もあります。件名に釣られて安易にメールを閲覧することの禁止、或いは本文中の URL をクリックしない、不審な添付ファイルを開かない、などの定着化を狙いとするサービスです。引っかかる人は年配者に多いと聞いていますので、人間系による防御力や「目利き」の向上を検討されてはいかがでしょうか。

3. 保険代理店のPマーク新規取得に復調の兆し

Pマークニュース創刊の狙いは、Pマークの取得を検討している保険代理店のみなさまに個人情報保護に関する法制度・規格や情報セキュリティの動向について情報発信して、保険代理店のPマーク取得を後押しすることでした。

このため、弊社では約10年に亘って保険代理店のPマーク取得（保有）に関する動向をフォローして参りました。ここ数年は明るい話題が殆どなかったのですが、2021年を迎えて漸くPマーク新規取得の動向に復調の兆しが出てきました。

(1) 保険代理店におけるPマーク取得動向に変化の兆し

保険代理店におけるPマーク取得は、下表の通りです。

2018年頃までは下表の通り順調に増加傾向が続いていましたが、2018年にPマークの準拠規格である「JIS Q 15001」が改訂されたことから、所謂「新JIS対応」の困難さから、Pマーク取得に急ブレーキが掛かり、2019年および2020年のPマークを新規に取得した保険代理店は僅か3社という低調さに陥り、「保険代理店にもうPマークは不要なのか？」と思えるような氷河期を迎えていたのです。

項目	2015年	2016年	2017年	2018年	2019年	2020年	2021年
新規取得代理店数	16	15	11	7	3	3	7
更新取止め代理店数	5	4	2	13	7	6	3
年度増減数	11	11	9	-6	-4	-3	4

(注)2021年は8月現在

ところが、年が改まった今年（2021年）においては、8月までに新規取得代理店が7社を数えるといった状況になっています。新たにPマークを取得する保険代理店が、久し振りに年間10社を超えそうな勢いなのです。

(2) 2021年度にPマークを新たに取得した代理店

2021年に新たにPマークを取得した保険代理店は、下表の7社です。

	取得時期	所在地	保険会社取扱（乗合）状況	設立
A社	2021/1	東京都	損保2社	2015年
B社	2021/2	東京都	生保16社、損保13社、小短7社	2019年
C社	2021/2	大阪府	生保12社、損保1社	2018年
D社	2021/3	東京都	生保23社、損保7社	2006年
E社	2021/5	宮城県	生保6社、損保2社	2017年
F社	2021/6	東京都	生保14社、損保7社、小短4社	2010年
G社	2021/8	大阪府	生保21社、損保6社	2003年

上記7社がホームページにおいて発信している情報には限りがありますが、上表から窺えるのは、

- ①生保の営業活動を活発に行っている保険代理店が多い。
- ②設立が新しい（2015年以降の設立が4社）会社が目立つ。
- ③やはり大都市に営業基盤を持つ保険代理店が多い。

です。

やや乱暴な見方ですが、最近の保険代理店におけるPマーク取得動向は、「大都市圏で生保営業が厳しさを増しているなかで、これから事業の拡大を図る意欲的な乗合保険代理店の経営者が、企業ガバナンスの確立や他社との差別化を図るためにPマーク取得に向かってきた」ように思われます。

また、保険代理店のPマーク取得動向を見極めるうえで避けられないのが、「Pマークの継続更新を取止める保険代理店」についてです。こちらも2018年以降、心配な状況が目立ちましたが、今年は現状3社であり、この面でも保険代理店におけるPマーク保有の有効性が見直されていると評価されます。

(3) Pマークを取得するなら「今！」の時期を迎えています

数年前にも同じフレーズで訴えましたが、既に本誌でご案内の通り、改正個人情報保護法が2022年（4月）に施行されます。この法改正を受けてPマークの準拠規格であるJIS Q 15001も改定の運びとなることを見込まれています。再び「新JIS対応」が不可避となり、現状以上にPマークの取得は、負荷の多いものになることが予想されます。

即ちPマーク取得を検討されている事業者にとって、今が取得のチャンスという訳です。

そこで、本稿の最後に、保険代理店のPマーク取得における「期待される効果」を列記します。

- ①改正保険業法の「体制整備」義務として求められている「個人情報の取扱いに関する社内規則」が整備され、「顧客目線に立った代理店運営」に資することができる。
- ②個人情報保護法に対する体制が確立し、社会的責任が果たせる。
 - a) 個人情報の漏えい、紛失、改ざん、破壊及び盗難を防止できる。
 - b) 個人情報の取扱いに対する社会的信用が高まる。
- ③個人情報の取扱いに対する信頼感が高まり、企業イメージが向上する。
 - a) 企業外部への個人情報の取扱いが厳格に行われる。
 - b) 秘密に係る契約締結などに有利である。
- ④役員・従業員・委託先社員の個人情報保護に対する意識が高まる。
 - a) 個人情報そのものに対する意識が高まる。
 - b) コンプライアンス・プログラムの教育・遵守が達成される。
- ⑤プライバシーマーク（Pマーク）の使用により、個人情報取扱をアピールできる。
 - a) 名刺、封筒、便箋にプライバシーマーク（Pマーク）を入れられる。
 - b) ホームページにプライバシーマーク（Pマーク）を付けられる。
 - c) カタログ、宣伝広告資料などにプライバシーマーク（Pマーク）を入れられる。
- ⑥Pマーク運用が求めるマネジメントサイクル（PDCAサイクル）の実践は、代理店の業務活動における基本的なスタイルとなり、業務活動の活性化が期待できる。

4. お知らせ

トムソンネットを保険業務の様々な局面でご活用ください。

弊社は創業から17年が経過し、コンサルタントも40名を超えて、年々業務内容を拡充させております。

下表の通り幅広い分野において、みなさまのお力となることを願っております。

(各業務の詳細は弊社ホームページをご覧ください)

人材育成ソリューション	刊行物	保険ビジネス情報発信
<ul style="list-style-type: none"> ・ 損保講座／基本コース ・ 損保講座／上級コース ・ 損保特別講座 ・ 生保講座／基本コース ・ 生保講座／上級コース ・ 生保特別講座 ・ 生保損保・公開講座 	<ul style="list-style-type: none"> ・ 図説・損害保険ビジネス ・ 図説・損害保険代理店 ビジネスの新潮流 ・ 図説・生命保険ビジネス ・ 保険募集制度の歴史的転換 ・ 保険代理店にとっての 顧客本位の業務運営 ・ 変わり続ける保険事業 ・ 会社経営トップの 賠償責任と保険 	<ul style="list-style-type: none"> ・ 金融監督行政全般 ・ 保険募集制度 ・ 自動運転時代の到来と リスクと保険について ・ デジタル革命と 今後の保険ビジネス ・ 海外の保険業界動向
リスクマネジメント	ビジネスコンサルティング	システムコンサルティング
<ul style="list-style-type: none"> ・ P マーク取得支援 ・ システム監査支援 ・ 情報セキュリティリスク 対策評価・監査関連 サービス (TISAS) 	<ul style="list-style-type: none"> ・ 課題解決プログラム ・ 代理店ビジネス ・ 再保険ビジネス ・ アクチュアリアルサポート (保険数理関連業務支援) 	<ul style="list-style-type: none"> ・ 損保システムと事務 ・ 生保システムと事務 ・ 少額短期システムと事務

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おります。お気軽にどうぞ！

連絡先 株式会社トムソンネット (<https://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)