Ｐマークニュース

＜２０２０年陽春号＞　Vol. ３１

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

新型コロナウィルス感染の拡大は留まるところを知りません。そのため、世界中で現代科学の英知を集めた感染対策が展開されています。その対策の中で注目されるのが、個人情報を取扱う「デジタル追跡」アプリの開発・利用です。
記事では、「デジタル追跡」（新型コロナウィルス感染者追跡システム）の概要を紹介し、世界各国の取り組みや、導入効果とその課題について探っています。
また新型コロナウィルス関連として、個人情報保護委員会が公表している「感染症対策における個人データの取扱いについての考え方」も紹介しています。

JIPDEC が公表している 2018 年度の「個人情報の取扱いにおける事故報告集計結果」を見ますと、主要な事故原因として「メール誤送信」（586 件：25.2%）が最も多く、次いで「紛失」（478 件：20.6%）、「宛名間違い等による誤送付」（346 件：14.9%）の順となっています。ところがこうした事故原因の裏側には、共通的に真因ともいえる「うっかりミス」の存在があります。
記事では真因となる「うっかりミス」について分析し、その対策として「仕組みとしての再発防止策」を講ずることの必要性を説いています。
重大ミスを未然に防ぐためにも、みなさまのヒントになればと思います。

IT 資産の効率的活用と情報セキュリティの強化は重要な経営課題です。これらの適正な運用には、IT 資産と情報セキュリティに関する「社内の状況を知る」ことが不可欠です。一口に状況を把握すると言っても容易なことではありません。もはや手作業では不可能になりつつあるこの厄介な作業を、システムによって「見える化」し、状況把握の手助けをするのが、IT 資産管理システムです。
既に導入されている事業者さんもいらっしゃると思いますが、今回は IT 資産管理システムの機能や導入時のシステム選定や運用のポイントを紹介しています。

以上

1．新型コロナウィルス感染対策での個人情報利用を巡って
－「デジタル追跡」アプリの開発・利用―

広がる新型コロナウィルス感染は、留まるところを知りません。その感染対策が、現代科学の英知を集めて展開されています。その対策には「人・人感染」を阻止すべく、ネットワークを利用したいくつかの対応がみられ、当然のことながら個人情報を取扱っています。

新型コロナウィルスの感染拡大防止対策で利用される**「デジタル追跡」**を中心に個人情報取扱いの実態を通して、その効果と課題を探ってみました。

（1）携帯端末「位置情報」等統計データの利用

NTT ドコモの基地局データによる「密集地域などの人出状況分析」、また、いわゆる「コロナ疎開」状況の分析により特定地域での人の流れの追跡が行われ、その分析結果が報道されています。これらは、内閣官房、総務省、厚生労働省、経済産業省が連名で、プラットフォーム事業者・移動通信事業者等に、「外出自粛要請等の社会的距離確保施策の実効性の検証、クラスター対策として実施した施策の実効性の検証、今後実施するクラスター対策の精度の向上」のため、これに資する統計データ等の提供要請に基づいた（2020.3.31 付けの要請）ものであり、法令上の個人情報には該当しない統計情報等のビックデータの活用となります。

（2）携帯電話の位置情報を利用した「デジタル追跡」アプリの開発・利用

報道によれば(2020.4.20 朝日)、5 月上旬にも個人のスマホの記録を使った新型コロナウィルス感染者追跡システムが動き出すとのことです。政府が一般社団法人「コード・フォー・ジャパン(CFJ)」と開発中と伝えられます。利用者がアプリを取得すると、近距離無線通信「ブルートゥース」を通じ、他の利用者が一定距離内に近づいた履歴が携帯端末に記録され、後に利用者から感染者が出た場合、その利用者と至近距離にいた人に「濃厚接触者の可能性」について通知される仕組みです。「いつ、どこで、誰と接触した」かについては通知されません。利用者が自分で「陽性」と入力すると、いたずらされる懸念もあり、入力は「行政職員に限る」として、その処理は、利用者のスマホを預かって入力したりする方法、アプリに電話番号を登録してもらい、感染者の同意を得て電話番号を元に入力する方法等が想定されているようです。また、CFJ と行政の双方から、感染者の接触情報履歴や接触者のリストなどは見られないようにするということです。個人情報を取扱う「デジタル追跡」アプリの開発・利用です。

（3）世界で広がる「デジタル追跡」アプリの開発・利用

「デジタル追跡」アプリの開発・利用が世界各国で展開されていると報道されています(2020.4.20 朝日など)。

中国政府では、1 月 30 日、感染者の行動を追跡するビックデータ分析チームを立ち上げ、感染者が使った交通機関の便名や座席番号、駅や空港の出入場記録などを集め、その行動を

割り出してきました。メディアなどで感染者の詳しい移動経路を明かし、監視カメラの映像をもとにしたとみられる分刻みの動きも公表、同じ便に乗った人や濃厚接触者に申告を促す狙いで、全土で約72万5千人の濃厚接触者を追跡できたと説明しています。

韓国では「自主隔離安全性保護」と名付けられたスマホアプリにより、自宅待機を命じられた市民に、担当職員が連絡して健康状態を報告させ、さらにGPSを使用して自宅待機中の市民の位置情報を追跡し、隔離エリアから離れていないことを確認できるといわれています。

このスマホアプリを利用することで、自宅隔離者は担当職員に症状を報告し、状況の変化を伝えられるようになり、指定された隔離エリアから離れた場合は、隔離対象者と担当職員の双方に警告メッセージが送信されるとのことです。

台湾でもこの隔離措置の対象者を監視するスマホアプリが開発されました。「電子フェンス」と呼ばれるこのシステムは、対象者のスマートフォンの位置情報を監視し、対象者がその住所から離れると警察や当局に通知するというものです。また、スマートフォンの電源を15分以上切った際にも通知されるといいます。

香港で導入されたリストバンドは、隔離に耐えられなくなった患者が出歩かないよう監視するとのことです。リストバンド内部のICチップが患者のスマートフォンと連動し、異常を検知した場合、当局にアラートが送信されます。 香港政府は2月からこのオペレーションを開始し、わずか1カ月でリストバンドの量産体制を整えたといわれています。

欧州委員会は3月23日、域内のドイツ・テレコムやオレンジなどの大手通信事業者に対し、ユーザーの匿名化データを提供するよう要請しました。また、**日本**が導入を目指すシステムの必要性が語られ、英国、フランスで開発中とのことです。さらに**イスラエル**では3月17日、テロ対策用に開発された携帯電話追跡のテクノロジーを、30日間の時限措置として新型コロナウィルスの感染追跡目的にも使用することを明らかにしているといわれています。

（4）「デジタル追跡」システムの導入効果と課題

「デジタル追跡」システムの導入利用は効果を挙げています。その効果は、国情によって異なるその他の関連する諸施策も大きく影響していると思われるものの、「「デジタル追跡」システムをいち早く導入し実施してきた韓国」と「これから開発の日本」では、感染経路不明の感染者割合が大きく異なる結果として表れています。韓国 6%に対して、日本 72%(2020.4.17 時点)です。この事実は、早期感染収束に大きな影響を及ぼします。2020.4.22 現在のコロナウィルス感染回復率は、日本11.13%に対して、韓国76.88%、台湾81.06%、中国92.78%といわれています。(Mapping the Wuhan Coronavirus (2019-nCoV) 米国ジョンズ・ホプキンズ大学による。)

一方、マイナスの側面も見えます。新型コロナウィルス感染者を見つけ出そうとネット上では魔女狩りが始まり、社会に恐怖感が広まり、感染者情報の漏洩も起こっているようです。このテクノロジーを使うと、あらゆる携帯電話の位置情報、通話、メッセージなどを把握することができ、個人情報が想定外の目的外利用をされる不安もあります。

（5）「デジタル追跡」と個人の権利

国際人権規約は、新型コロナウィルス感染拡大という「生存を脅かす」場合は、個人の権利を制約できるとしています。政府も「新型インフルエンザ対策特別措置法」として法制化しています。個人情報保護という個人の権利についても同様と思われます。個人情報保護委員会は、「感染症対策における個人データの取り扱いについての考え方」として、下記を公表しています。(2020.4.2)

> 個人情報取扱事業者は、保有する個人データについて、原則として、本人に通知等している利用目的とは異なる目的で利用し、又は、本人の同意なく第三者に提供することは禁じられています。しかしながら、以下に該当する場合には、例外として、**本人の同意を得ることなく、目的外利用や第三者への提供が許され、**今般の新型コロナウィルス感染症の 感染拡大防止に当たっては、これらの例外の適用も含めて対応することが可能です。
>
> **1）**国の機関等からの情報提供の要請が、当該機関等が所掌する法令の定める事務の実施のために行われるものであり、個人情報取扱事業者が協力しなければ当該事務の適切な遂行に支障が生ずるおそれがあり、かつ、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるときは、当該事業者は、自らの判断により、本人の同意なく、個人データを目的外に利用し、又は当該機関等に提供することができます（本法第 １６条第３項第４号、第２３条第１項第４号）。
>
> **2）**人の生命、身体又は財産の保護のために必要がある場合や、公衆衛生の向上のために特に必要がある場合であって、本人の同意を得ることが困難であるときも、個人情報取 扱事業者は、本人の同意なく、個人データを目的外に利用し、又は国の機関を含む第三 者に提供することができます（本法第１６条第３項第２号及び第３号、第２３条第１項 第２号及び第３号）。

また、「社員に新型コロナウィルス感染者と濃厚接触者が出て、社内公表する場合、仮にそれが当初特定した利用目的の範囲を超えていたとしても、当該 事業者内での２次感染防止や事業活動の継続のために必要がある場合には、**本人の同意を得る必要はない**」こと。更に 「社員が新型コロナウィルスに感染し、当該社員が接触したと考えられる取引先にその旨情報提供することも、**同様に、本人の同意を得る必要はない**」とコメントしています。

ただ、新型コロナウィルスの感染拡大という非常事態への対処を理由として、追跡・監視に大きく振れる動きが広がりかねず、これが常態化するのではないか、という懸念も指摘されます。とりわけデジタル監視を加速させている中国について、リーマンショック後の後戻り不能な世界経済を指して使われた「ニューノーマル（新常態)」という言葉で、監視による人権侵害はすでに“ニューノーマル”となっている、と指摘する中国人識者もいます。

「デジタル追跡」アプリの開発・利用により人権侵害が助長されることになるか否かは、国情によって異なり「政府への信頼感」により左右されそうです。ドイツのメルケル首相は「デジタル追跡」アプリの開発・利用について、ナチスや旧東欧の経験から「市民が自発的に導入するのが前提だ」と強調しているといわれます。「デジタル追跡」システムの導入利用は、「命を守る戦い」に効果を挙げています。その事実を踏まえて、「デジタル追跡」アプリが、「監視の恐怖」を生むことなく「保護されている安心」を生み、直面するコロナ禍の収束にプラスになるよう、その開発・導入・利用にあたっては、我国での**丁寧な説明と透明性の確保**が強く望まれます。

２．事例に学ぶ：「うっかりミス」は予防できないのか

事例シリーズの第８弾になります。今回は情報セキュリティの中で頻発する「うっかりミス」について考察してみたいと思います。

プライバシーマーク制度の総本山に当たる JIPDEC は毎年秋口に「個人情報の取扱いにおける事故報告集計結果」を公表し、注意を喚起しています。その最新版（2018 年度実績）に〝事故の原因を件数が多い順に見ると、「メール誤送信」（586 件：25.2％）が最も多く、次いで「紛失」（478 件：20.6％）、「宛名間違い等による誤送付」（346 件：14.9％）となりました〟と紹介されていますが、この数年ワーストスリーは変わらない状況にあります。

ここで〝（事故の）原因〟とありますが、これはこの稿においては〝事象〟と言うべきで、原因（〝真因〟）は別のこととして取り上げます。**真因を追究し本当の意味での再発防止**に繋げていただければと考えるが故です。

（１）参考となる事例

①製造会社の例

知人に製造会社の社員がいます。当人の新入社員時代に生産ラインの実習があり、不注意で工具を落としラインを止めたことがあったとのことです。

即座に工区の全員が集結したため、白い目で見られ厳しい叱責を覚悟しましたが、案に相違してみんなは工具が落ちた原因を討議し始め、手の動きがぎこちなくても工具が落ちること自体を問題（真因）と結論付けたようです。

業務が終了した後、作業台のヘリにガードを取り付けたことで、以降工具の落下が再発しなくなりました。この会社は事務系の業務を含む全社レベルで、ミスがあっても決して当人を責めず原因を〝なぜなぜ〟と深掘りする習慣が根付いており、従ってミスを隠すことがないと聞き敬服した記憶があります。

②広告会社の例（テレビドラマ）

2019 年 3 月に放映されたドラマ「わたし、定時で帰ります。3 話」を大変興味深く観ました。

あらすじを簡単に述べると、広告会社の新入社員が CM 撮影の休憩時間に出演者の私的な会話風景をスマホに隠し撮りし、動画をグループチャットに送ったところ友人が SNS にアップし炎上したのが発端（事実＝事象）で、その対策に主役の先輩女子社員が奮戦した、と言うストーリーです。結果はハッピーエンドでしたが、ハラハラさせられました。

個人情報保護の視点では「出演者の個人情報の目的外利用、及び同意を得ずしての第三者提供（Web での公開）」となります。

一般に、原因は新入社員の〝認識不足〟とし、対策は〝再教育〟としているケースが多いのではないでしょうか。このドラマでは〝なぜ当人が無断で撮影したか〟、更にその背景は？　と再三に亘り当人にヒアリングを行い、真因を探求して行きます。

最終的には、新入社員が自信を喪失している中でついついやってしまったのが実態で、会社として日頃の本業での指導が疎かだったことを真因としていました。対策は通り一遍の〝教育〟ではなく、先輩社員の責任指導体制を採るようにしました。

③プライバシーマーク事業者の例

個人情報に関する事故例のトップにある「メールの誤送信」対策のため、自動メール配信システムを導入した会社があります。顧客 DB を利用し、メールの宛先と本文の冒頭に書く社名と氏名をシステム機能で生成させることを図りました。言ってみれば、「Word」の「差し込み印刷」のような機能です。

システムの導入はしても、外部へのメール（本文）は上司の査読を得ること、複数の宛先に送る場合はプレビューで現物を確認すること、などのルールを定め周知をしていたのですが、誤送信が発生しました。本文中の宛先（会社名、氏名）を顧客 DB からもたらされるべくパラメータを書かないといけないにも拘わらず、先頭の宛先のものをそのまま記入したため、120 件のメールは同じ〝○○会社○○○○様〟で始まってしまいました。「個人情報の漏洩」です。

ルール通りの手順を踏んだのですが、プレビューしたのは最初のメールだけだったことでパラメータにしていないことに気づかなかった訳です。原因は〝急いでいたため〟としました。でも、なぜ急いでいたのかは未解決です。

（2）〝うっかりミス〟の分析

上の例は全て〝うっかりミス（ケアレスミス）〟と言えると思います。後日、当人は頭では分かっているのにどうしてあんなことを、と猛省したことでしょう。

人事部長向け専門誌「日本人材ニュース」ではうっかりミスを次の 4 つのタイプに分類し対策を示唆しています。

ミスのタイプ	ミスの説明	例	対策
①省略エラー	すべきことを忘れてしまうミス	会議を忘れた	仕事の手順やすべきことを整理する
②実行エラー	不要なことをしてしまうミス	必要なファイルまで廃棄した	誰か別の人にチェックをお願いする
③不注意エラー	無意識的に起こるミス	茶碗をひっくり返した	行動を起こす前にひと呼吸おく
④思い込みエラー	勘違いや早とちりのミス	アポの時間を取り違えた	間違いや認識のズレがあるものと思っておく

別な切り口での統計によると、ケアレスミスを犯す人の特徴として〝体調管理が苦手〟がトップに来るようです。次が前項の(2)のような〝悩みを抱えている〟が続きます。

体調が思わしくない時や悩みがある時に対外的な影響のある作業を行う際には、自分に〝**今日はきっとミスを犯すはず**〟と言い聞かせてはいかがでしょうか。

更に、〝思い込み〟を予防するには「見える化」をお勧めします。Windows 標準で「付箋」アプリがありますから、大事なことを画面に常時表示させることができます。

（３）ミス（失敗）を改善へのヒントに

「トヨタの失敗学」では冒頭、〝「失敗」とは改善へとつなげるチャンスであり、成果に結びつける「宝の山」〟と述べられています。つまり、ミスを人ではなく仕組みの問題と捉えて原因を知り、共有（**「視える化」・「横展」**）し、精神論で終わらせない、の意味です。そして改善した結果が積もり積もって「品質を工程でつくり込む」ことに成功しています。

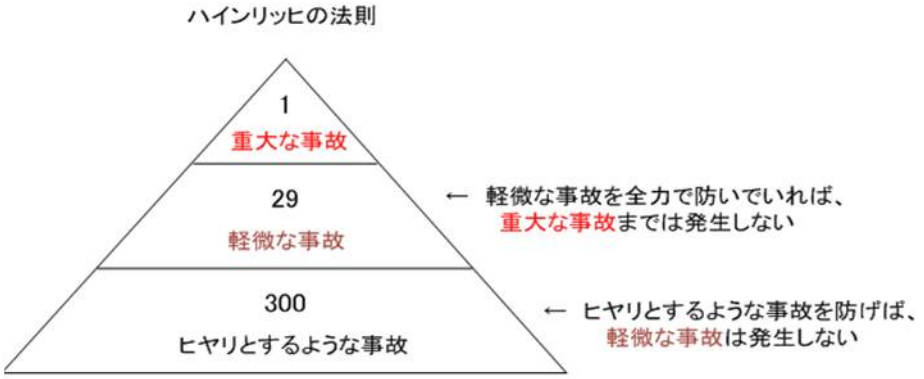
人間は過ちを犯す存在です。真因を間違えると対策が的外れになります。つまり、真因を探り対策を心に刻む、できれば(3)のように業務環境の仕組みとしてシステムの導入などの再発防止策を整備したいものです。

プライバシーマーク審査において多くの会社で指摘される事項は、①個人情報の特定漏れ、②委託先の認識漏れ、③リスク分析で業務の流れと相違している、がワーストスリーです。多くの会社の改善報告書では「原因」に〝失念していた〟〝洗い出しに緻密さが欠けていた〟などが挙げられ、「対策」は〝追加特定した〟などが書かれています。一方ではしっかりと真因を探り、仕組みとして再発防止策が講じられていて大変頼もしく感じられたこともあります。

（４）終わりに

目下、在宅ワークを強いられている人も多いことと思います。会社の環境とは違って仕事に関係のない音が聞こえたり、ともすれば緊張感がやや希薄になることを懸念します。このような時こそミスを犯さない訓練の好機と捉えることができます。

多くの会社では個人情報の取扱い上でのミスは会社の致命傷にはならないでしょう。しかし、「ハインリッヒの法則」を思い起こせば、些細な事象と思われることであってもそれを安易に見過ごすことが職場の体質になり、ひいては**本業（基幹業務）における重大事故の遠因**になることを最も恐れます。「禍を転じて福と為す」を祈念して已みません。



３．IT 資産と情報セキュリティの管理（見える化）はシステムにお任せ

多くの企業では IT 資産の最適化や情報セキュリティ対策の強化、更には適切なライセンス管理等々、従前にも増して IT 資産と情報セキュリティの管理の充実が、企業経営にとって重要な課題になっています。

この IT 資産管理や情報セキュリティ管理の増大、複雑化に伴って、対応が人手では追い付かず、適切な状況把握と管理が難しくなっています。こんな状況に対処するために生まれたのが、企業内の IT 資産等をシステムで管理しようとする IT 資産管理ツールです。

以下では IT 資産管理システムの概要、導入における検討ポイントを纏めてみました。

（１）IT 資産管理システムの仕組み

IT 資産管理ツールの仕組みは、PC 等の各機器にエージェントと呼ばれるソフトウエアをインストールして、サーバーで情報を集約管理するのが一般的です。最近はサーバーではなくクラウド上で集約管理するタイプも多くなっています。

PC 等に配されたエージェントは、当該 PC の機器やソフトウエアに関する管理情報などを定期的に収集して、管理サーバーに情報を送ります。管理サーバーでは収集情報を蓄積しつつ、情報を分析して、違反や脆弱性などあれば、管理者にレポートします。

（２）IT 資産管理システムにおける取得情報および管理対象について

IT 資産管理システムは、以下に示す多様な情報取得と運用の状況把握を行います。

①IT 資産情報を収集して IT 資産運用を最適化

取得情報区分	取得情報
ハードウェア情報の取得と台帳管理	コンピュータ名、IP アドレス、CPU の種類、メモリ容量、ディスク容量などのハードウェア情報を自動的に取得する
ソフトウエア情報の取得	OS のバージョン、アップデートの適用状況、コンピュータ内部にある実行形式ファイルなどの情報を自動的に取得する
更新プログラム管理と適用	Windows 更新プログラムやセキュリティパッチの適用状況を把握し、必要な更新プログラムを一斉に適用する
周辺機器情報の取得	ネットワークに接続されているプリンタ、複合機、ルーター、スイッチなどの周辺機器情報を自動的に取得する
デバイス情報の取得	USB メモリ、光ディスクドライブ、デジタルカメラ、スマートフォンなどのデバイス情報を自動的に取得する
死活監視	プリンタやルーターなどの死活監視を行う

②ソフトウエア資産管理（SAM）によるライセンス適正化

処理区分	処理の内容
管理台帳の作成	ソフトウエア資産管理に利用する管理台帳を作成する。 （ライセンス情報の登録／割当、資産の棚卸しなどを行う）
ライセンス登録	ソフトウエアのライセンス数／種別、使用／管理部署など必要な情報を登録する

処理区分	処理の内容
ライセンス利用状況	保有ライセンス数とインストール数の過不足確認、アップグレード／ダウングレードなどの利用状況を把握する
不要ソフトウエア廃棄	ライセンス超過やライセンス切れなどにより不要になったソフトエアをチェックする

③セキュリティ対策の強化

機能区分	機能内容
ログ管理	アプリケーションの起動状況や外部との通信、特定のファイル操作、データの取り扱いなどコンピュータで実行された様々な挙動をログとして記録し、管理する
アカウント管理	業務アプリケーションや Web サービスなどのアカウント状況を把握する
ネットワーク検知	ネットワークの接続状況を監視して情報収集を行い、管理対象外の不正な機器接続を検知、遮断する
操作制限	ファイルのアップロード、メール送信、印刷出力などの操作をクライアント コンピュータ単位、ユーザー単位で制限する
アラート表示	違反行為があった際に、メッセージを送信してユーザーに注意を促す
サーバー／データベース監査	サーバーのログを収集し、権限のないユーザーからのアクセスやデータベースの使用状況などを把握する
レポート	サーバーやフォルダ、ファイルへの失敗アクセス状況をレポートとして可視化する

（3）IT 資産管理ツールの選び方

IT 資産管理ツールには上記の通り多様な処理機能が含まれますが、製品によって搭載されている機能が異なりますので、事前の調査と慎重な選択が必要になります。

システム選定におけるポイントを集約すれば以下 3 点となります。

■オンプレミス型かクラウド型か

■自社が必要とする管理機能が搭載されているか

■求めるセキュリティレベルを維持できるか

（4）システム運用時の留意点

IT 資産管理システムは、システム導入しさえすれば、IT 機器や情報セキュリティに関する管理が自動的に適切に運用出来るようになる訳ではありません。

実際にシステムを稼働させて、その結果としてシステムが収集した情報やデータの内容、あるいはシステムから報告されるメッセージを、システム担当者がしっかり把握し、対処するという、システム運用の部分が非常に重要です。

特に、IT 資産管理に係る専任の担当者をアサインできない場合は、日々短時間（10 分程度）の運用でセキュリティ状況やシステムの稼働状況の概略を把握出来ることが肝要です。

このため、IT 資産の状況や情報セキュリティの遵守状況の「見える化」がしっかり出来ているシステムが、お勧めと言えます。

４．お知らせ（トピックス）

（１）2020 年 3 月末の P マーク取得事業者数は **16,477** 社でした。

JIPDEC より 2020 年 3 月末の P マーク取得事業者数が発表されました。

時期	2018/3/31	2018/9/30	2019/3/31	2019/9/30	2020/3/31
P マーク取得事業者数	15,788 社	15,969 社	16,275 社	16,346 社	16,477 社
半期増加数		181 社	306 社	71 社	131 社

上記の通り 2019 年度（2019 年 4 月 1 日～2020 年 3 月 30 日）における一年間の P マーク取得事業者数の増加は、新 JIS 対応等の影響から 202 社と例年の半分以下に留まっています。

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。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）