Ｐマークニュース

＜２０２１年新春号＞　Vol. ３４

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

昨年８月経産省から「プライバシーガバナンス　ガイドライン V1.0」が公表され、今、「プライバシーガバナンス」が注目されています。企業が顧客データをはじめとするパーソナルデータを取り扱おうとするとき、個人情報保護法の遵守はもちろん、プライバシー保護の観点から十分な対策を講じておく必要があります。

そこで「プライバシーガバナンス」に関して、「プライバシー情報って？」「プライバシーガバナンス　ガイドライン V1.0 の提言」「事業者に求められること」についてまとめて解説しました。

JIS 規格（JIS Q 15001:2017）では「組織は、認識させる手順に、全ての従業者に対する教育を少なくとも年一回，適宜に行うことを含めなければならない」と教育の実施を規定しています。

この「教育」に近い存在に「研修」があります。教育は「ある人間を望ましい姿に変化させるために、身心両面にわたって、意図的、計画的に働きかけること」で、研修は「職務上必要とされる知識や技能を高めるために、ある期間特別に勉強や実習をすること」と理解されますが、両者の違いを掘り下げつつ、JIS 規定における認識＝教育の問題を考えて見ました。

昨年は年間を通してコロナ禍のために、仕事面でもプライベートにおいても色々大変な苦労を強いられました。そんな困難の多かった 2020 年は、セキュリティ関連でも、従来とは異なる新しいタイプの事件や動向が現れた年でした。

日本ネットワークセキュリティ協会（JNSA）が昨年の暮れに発表した「2020 年セキュリティ 10 大ニュース」で、2020 年を振り返ると、我々は、そこに「コロナがもたらした大変革時代の幕開け」を思わせる新たな動きを見出すことになります。

以上

１．「プライバシーガバナンス」を巡って

―　個人情報保護法の範囲を超える「パーソナルデータ」の利活用　―

Society5.0 を見据えて「パーソナルデータ」について、「プライバシーガバナンス」が必要であるとして、そのガイドラインが公表されています。2020 改正個人情報保護法では、データの利活用として、「仮名加工情報」「個人関連情報」を新たに定義していますが、そのガイドラインが、まだ未公表のため、詳細が把握できません。今回は「個人情報」から視野を広げて、「パーソナルデータ」とりわけ「プライバシー情報」にかかわる課題の状況、内容、必要と思われる事業者の対応について考えます。

＊＊Society 5.0

サイバー空間（仮想空間）とフィジカル空間（現実空間）を高度に融合させたシステムにより、経済発展と社会的課題の解決を両立する、人間中心の社会（Society)。

狩猟社会（Society 1.0)、農耕社会（Society 2.0)、工業社会（Society 3.0)、情報社会（Society 4.0）に続く、新たな社会を指すもので、第５期科学技術基本計画において我が国が目指すべき未来社会の姿として初めて提唱されました。

（1）「プライバシー情報」って？

IoT（Internet of Things）、AI(人工知能、Artificial Intelligence)やビッグデータなどのデジタル技術が進展するに伴い、データの利活用への期待が大きく膨らむ一方で、「パーソナルデータ」の利活用にあたって、プライバシーの観点から社会からの批判を避けきれず炎上したり、それにより企業がデータの利活用を躊躇するケースも見られます。法令を遵守していても、本人への差別、不利益、不安を与えるとの点から、個人や社会からの批判を避けきれずに炎上し、さらにそれが、当該事業に多大な影響を与えるケースです。

**「パーソナルデータ」とは(「個人情報保護法に規定する『個人情報』に限らず、位置情報や購買履歴など広く個人に関する識別性のない情報も含む データ」（経産省パーソナルデータ WG 報告書))

「プライバシーガバナンス ガイドライン V1.0」（経産省 総務省 2020.8.26)には、例えばカメラ画像について、「データ利活用の拡大」がすすむとともに、一方で、そのプライバシーに関する懸念があることが、以下のように報告されています。

「カメラ画像は、防犯目的での利用だけでなく、例えば、店舗での人数カウント、来店客の性別・年代などの属性推定、リピーター判定といったスマートな店舗運営や購買体験を実現するという商用目的にも、公共空間での人流の把握、車載カメラ画像（個人の写り込み可能性のある画像）の分析による路面や構造物の状態分析などといった、スマートな街づくりを実現するという公共性の高い目的にも、幅広く貢献する可能性が見えてきていた。一方で、カメラ画

像は、個人の顔・全身が映り込みうる情報であり、顔画像や識別に必要となる生体情報は、一度取得されると将来にわたる追跡が可能となることや、流出してしまうと消去が困難になるとの認識から、個人が嫌悪感や監視への恐怖感を抱くケースが少なくない。実際に、カメラ画像を活用して人流計測を行う実証実験が、「顔追跡『やめて』」「監視社会」などの文脈から批判的な報道等により、中断・縮小しての実施となるケースも見られた。」

このように、従来の「プライバシー情報」に関する認識は、そのポイントが「私生活をみだりに公開されない法的保障ないし権利」や「放っておいてもらう権利」の確保から、「自己情報のコ ントロール」へと移っていると言われます。

**「プライバシー情報」とは、①個人の私生活上の事実、またはそれらしく受け取られる可能性のある情報、②公知になっていない情報、③私人としての立場に立つと公開を望まない内容の情報、のすべての条件を満たす情報。(三島由紀夫「宴のあと」事件(元外相有田八郎 VS 新潮社)での東京地裁の判断基準(1964 年 9 月 28 日)

（2）「プライバシーガバナンス ガイドライン V1.0」の提言

「IoT や AI の技術進展に伴って、データ解析の結果、機械的に不当な差別的扱いを受ける可能性や、個人の政治的選択に対して介入される可能性など、プライバシー問題は多様化している。企業には、Society5.0 に向けては、イノベーション推進の中心的存在として、積極的に経済的価値・社会的価値を創造する取組を推進すると同時に、プライバシーに関わる問題をはじめとする、イノベーション自体がもたらすリスクの低減を図っていくことが求められる。

企業は、**サイバー空間を介していても、取り扱うのは単なるデータではなく、フィジカル空間の生身の人間と向き合っていることを改めて認識し、個人の基本的な人権や社会的価値を損なうことのないよう、真剣に考えを尽くすことが必要**とされる。」

**「機械的に不当な差別的扱い」を受けるケースとは、例えば、偏ったパーソナルデータを利用して、プロファイリング(パーソナルデータを集めてコンピューターで自動的に解析し、個人の性向や属性などを推測・予測する手法)し、人が介入しないオンライン上で、借入申込やインターネットでの採用活動を行うなどのケースがあります。

更にその取り組みのポイントとして、経営者が取り組むべき三要件を下記としています。

① プライバシーガバナンスに係る姿勢の明文化
(プライバシーステートメントや、組織全体の行動原則などを策定)
② プライバシー保護責任者の指名
③ プライバシーへの取組に対するリソースの投入
(必要十分な経営資源（ヒト・モノ・カネ）を継続的に投入)

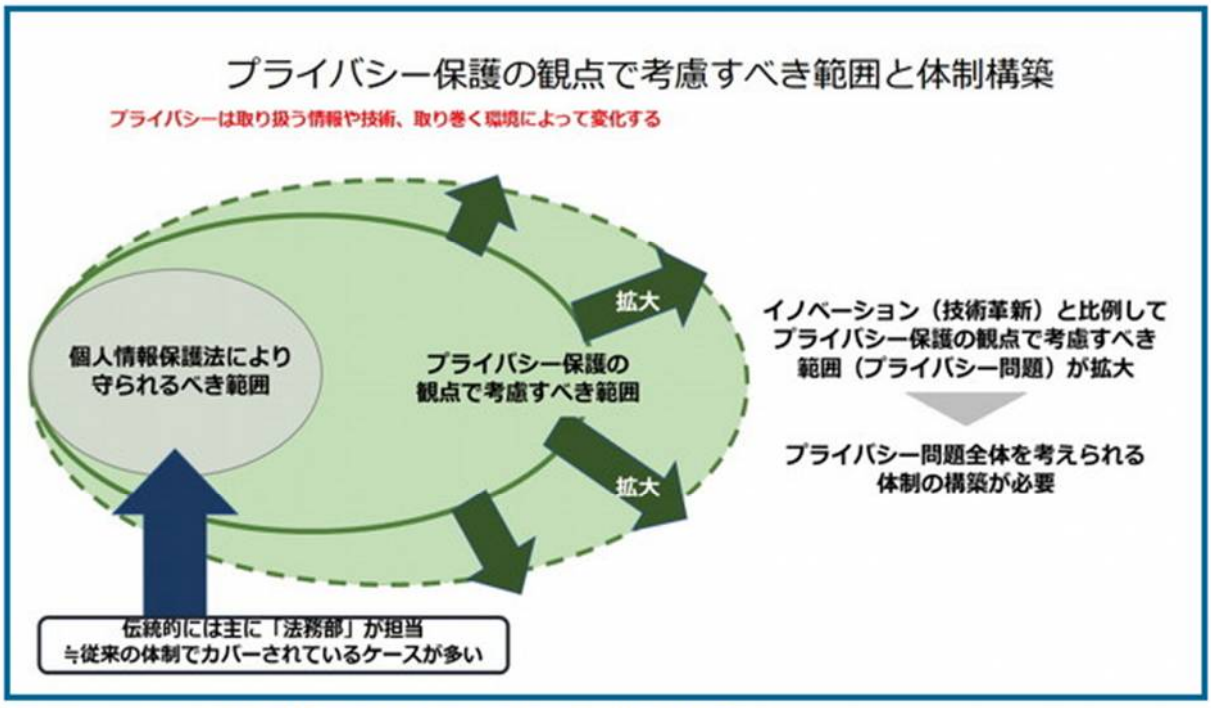
また、そのために必要な重要事項として 5 点を挙げています。

① 体制の構築(内部統制、プライバシー保護組織の設置、社外有識者との連携)
② 運用ルールの策定と周知(運用を徹底するためのルールの策定、組織内への周知)
③ 企業内のプライバシーに係る文化の醸成 (個々の従業員がプライバシー意識を持つよう企業文化を醸成)
④ 消費者とのコミュニケーション(組織の取組について普及・広報、消費者との継続的なコミュニケーション)
⑤ その他ステークホルダーとのコミュニケーション (ビジネスパートナー、グループ企業等、投資家・株主、関係行政機関、業界団体、従業員等とのコミュニケーション)

(3) 事業者に求められること

端的に言えば、**企業ガバナンスとしてのプライバシーガバナンスが必要**ということです。必ずしも個人情報保護法などの法令等遵守の範囲にとどまらない形で、プライバシー保護を、単なるコンプライアンス(法令等遵守)として受動的に対応するのでなく、組織全体として能動的に対応し、顧客やステークホルダーへ積極的に取組を説明し、社会からの信頼を獲得していくことです。

「金看板の保険代理店」は、まさに契約者の生命・財産の状況といったプライバシー情報を承知しており、顧客・契約者のプライバシー保護に、単なるコンプライアンス(法令等遵守)として受動的に対応するのでなく、その信頼と信用を獲得すべく、積極的に対応すべきでしょう。個人情報保護法の遵守に加えて、対応には、更に負荷がかかることになりますが、その対応の負荷は企業価値向上やビジネス上の優位性につなげていく、という企業の差別戦略と捉えたら如何でしょうか?



プライバシーは取り扱う情報や技術によって変化する(出展:総務省)

２．事例に学ぶ：「教育」について

事例シリーズの第 11 弾になります。本稿では「教育」について考えてみたいと思います。

そろそろ各社におかれては新年度の計画を立案する時期に差し掛かっているかもしれません。実は、以前から JIS 規格が求めている〝年一回の教育〟について実効性の面でやや疑問を抱いていたこともあり、一緒に考えていただければ幸いです。

（1）プライバシーマーク事業者における〝認識〟（教育）の義務

JIS Q 15001:2017 では以下のように規定されています。

《本文(本体)》

> 7.3　　認識
> 組織の管理下で働く人々は，次の事項に関して認識をもたなければならない。
> a)　内部向け個人情報保護方針及び外部向け個人情報保護方針
> b)　個人情報保護パフォーマンスの向上によって得られる便益を含む，個人情報保護マネジメントシステムの有効性に対する自らの貢献
> c)　個人情報保護マネジメントシステム要求事項に適合しないことの意味

《附属書 B》

> A.3.4.5　　認識
> 組織は，従業者が 7.3 に規定する認識をもつために，関連する各部門及び階層における次の事項を認識させる手順を確立し，かつ，維持しなければならない。
> a)　個人情報保護方針(内部向け個人情報保護方針及び外部向け個人情報保護方針)
> b)　個人情報保護マネジメントシステムに適合することの重要性及び利点
> c)　個人情報保護マネジメントシステムに適合するための役割及び責任
> d)　個人情報保護マネジメントシステムに違反した際に予想される結果
> 組織は，認識させる手順に，全ての従業者に対する教育を少なくとも年一回，適宜に行うことを含めなければならない。

このことから、〝年(年度)に一回、a)～d)を周知する〟ことを主眼にした〝教育〟を行っているケースが多いのではないでしょうか。とすれば、毎年同じ内容にならないでしょうか？

（2）〝教育〟と〝研修〟の違い

〝教育〟は「ある人間を望ましい姿に変化させるために、身心両面にわたって、意図的、計画的に**働きかけること**」で、〝研修〟は〝職務上必要とされる知識や技能を高めるために、**ある期間**特別に**勉強や実習をすること**。また、そのために行われる講習〟(いずれも「Goo 辞書」から)とあります。

この説明では主体は、教育が会社で、研修が本人(従業者)となり、述語は教育が「する」で研修が「受ける」が適切でしょう。更に、時期や期間に関しても、研修が〝ある期間〟としているのに対して教育にはそのようなニュアンスがありません。教育は期間を明示的に決めることなく、場合によっては日常的に行うことを含んでいると解釈できます。

従って、JIS 規格で〝少なくとも年一回,適宜に行うこと〟としているのは〝教育〟ではなく〝研修〟ではないかと思います。そのため、以降ではこの 2 つを分けて稿を進めてみます。

（3）〝教育〟と〝研修〟の例

「P マークニュース＜2020 年陽春号＞Vol. 31」でも紹介しましたが、TV ドラマ「わたし、定時で帰ります。3 話」で、広告会社の新入社員が収録現場において休憩中の出演者を撮影し SNS にアップして炎上したことがテーマになっていました。これは、個人情報保護の見地で言えば「本人の同意を得ずして個人情報(顔の映像)を第三者提供(一般公開)した」ことに該当します。当然法令違反です。

会社として原因を追及し再発防止策を講じることになりますが、採った策は〝研修〟ではなく〝教育〟でした。先輩社員をトレーナーに就け本来業務に自信を持たせる方策を講じました。個人情報(場合によっては機密情報)の公開の社内ルールを説いて終わりにせず、日常の仕事を通して情報の価値や取扱いのキーポイントを身に付けさせた訳です。

次に、ドライバー社員数百人を抱えるある運送会社では、事務や管理的な仕事をしている社員と違いドライバーにとって 10 数ページのテキストを読了するのは苦痛との声が上がり、しかも殆ど遭遇する場面がないことが述べられているため意味がないと判断しました。代替として、元々「社是」と「注意事項」を印刷したカードを渡し携行するように指導していることから、「注意事項」に少し PMS ルールを加え PMS 事務局の連絡先を印字し、配布の際に上長から補足説明もするようにしました。内容は毎年少しずつ更新をして陳腐化を防いでいます。実務と個人情報保護教育が一体化している格好のケースです。

一方、ある P マークの審査の場で相談を受けた会社があります。定期研修において JIS 規格「附属書 B」A.3.4.5a)～d)をクリアせんがために保護法や社内規程などの解説を中心に行ったところ、限定的な個人情報しか扱う場面がない役員や社員から〝明日から何をしたらいいの？〟との質問が寄せられ、担当者は返答に苦慮したとのことです。実効性に乏しい教育だった、と言えます。「附属書 B」に〝関連する各部門及び階層における〟とあるように、担当業務によって研修の内容も変えて然るべきです。

（4）〝教育・研修〟と〝運用の確認〟

教育を日頃の行動と結び付けて実施するとした場合、思い起こさせるのは「運用の確認」(《附属書 B》A.3.7.1)です。

要求されている事項は〝定期的に、及び適宜にマネジメントシステムが適切に運用されているかを確認〟することですが、これは「認識の具現化の確認」と解釈できると考えます。言い換えると教育そのもの、或いは理解度の確認に相当します。

上記の運送会社では、「運用の確認」で Google フォームのアンケート収集機能を利用し「注意事項」の遵守状態を自己申告しています。

チェック項目には「取り扱っている個人情報それぞれの利用目的を認識していること」「個人情報の取扱いに関して疑義が生じた場合の連絡先を承知していること」なども含みます。JIS 規格で要求されている〝a) 個人情報保護方針〟〝c) 個人情報保護マネジメントシステムに適合するための役割及び責任〟の一部に該当します。(保護方針と体制図の全体は事務所に張り出しています)

(5) 終わりに

JIS 規格(15001)では個人情報の保護活動として求められる事項が箇条として列挙されていますが、それらは独立している訳ではなく関連していることを理解し効率的に運用することが期待されます。個人情報の特定から始まり、リスク分析→研修→運用の確認(自己・自主点検)→内部監査→マネジメントレビューを一連のものとして捉えることを提案します。

そのことにより事務局や担当者の負荷が軽減・抑制されるだけではなく、従業者の皆さんの意識としても各種の定期的アクションが密接に連携し、ストーリーを持っていることに気付かされると思います。結果、個人情報や機密情報の取扱いが適切に維持されるのに加え、情報主体の本人をリスペクトすることまで繋がればベストと思います。

３．セキュリティ１０大ニュースで振り返る２０２０年

昨年は、コロナに明けコロナに暮れた 1 年でした。世の中全体がコロナ禍に覆われた状況が続く中で、セキュリティ関連においては、従来とは異なる新しいタイプの事件や動向が見られた年でもありました。

そんな一年を日本ネットワークセキュリティ協会（JNSA）が昨年の暮れに発表した「2020 年セキュリティ 10 大ニュース」で振り返ってみると、事件や事故だけではなく、我々はそこに「コロナがもたらした大変革時代の幕開け」の兆しを見出すことが出来ます。

以下、JNSA 発表の「2020 年のセキュリティ 10 大ニュース」を眺めてみます。

順位 （時期）	事象の概要
第 1 位 （4 月）	**新型コロナ感染症　7 都府県に緊急事態宣言** 新型コロナウイルスは、現在社会の人生の価値観、生活様式に大きな変容を促しました。勤労者／組織にとっても働き方の革命が求められ、2020 年はテレワークが急速・劇的に浸透した年となりました。特に 4 月に緊急事態宣言が発せられた以降、多くの企業においてテレワークの導入が急速に進み、テレワーク時代に対応するセキュリティ対策として、ゼロトラストが注目を浴びました。
第 2 位 （9 月）	**ドコモ口座サービスで不正使用発覚** NTT ドコモの電子決済サービス「ドコモ口座」を使って銀行の預金が不正に引き出された事件です。その被害は銀行が 11 行、被害件数は約 130 件、被害総額は約 3,000 万円に及びました。 大手通信事業者ドコモと銀行との組み合わせで提供されたサービスでこのような不正事態が発生し、ドコモと無関係の銀行利用者までもが被害者となる可能性があるなど、電子取引に大きな不安を与えました。
第 3 位 （9 月）	**「デジタル庁」21 年に設置へ** 9 月に発足した菅内閣は、コロナウイルスの感染拡大で露呈した政府・自治体のデジタル化の遅れに対処すべく、2021 年秋までに「デジタル庁」の新設を発表しました。国民に利便性の高い行政システムの提供を目指すと同時に、日本全体の DX の進展においての司令塔の役割を果たし、官民ともに俊敏で効率性の高い運営をできるよう IT を通じて導くという目標を掲げており、早期実現が期待されます。
第 4 位 （10 月）	**東証システム障害で終日売買停止** メモリー障害時の自動切り替えの動作不良によって惹起した、東証システムの障害は、東証の取引が終日停止したことで約 3 兆円規模の売買機会が失われたと言われ、さらに証券取引所はリアルタイムで世界経済とも連動していることから、社会に及ぼす影響は極めて甚大ものとなりました。 大規模な社会的システム障害時の影響の大きさを改めて考えさせられました。

第 5 位 （9 月）	**進化を続けるマルウエア「Emotet」感染急増** Emotet の主要な感染経路は添付ファイル付メールです。その感染手段は、添付ファイルを開かせた上でファイルに仕込まれた悪意のあるマクロを実行させるという、古典的な手法でした。Emotet はウイルス対策製品の検出を擦り抜け、あたかも正当な送信者からの自然なメールを装い添付ファイルを開かせる、といった非常に巧妙な手口が強力な感染力の要因となり、2020 年には数回に亘って猛威を振るいました。
第 6 位 （2 月）	**防衛関連企業、不正アクセス事案の調査結果を公開** 三菱電機への不正アクセスについて同社情報によれば、攻撃者が「ウイルス対策サーバー」の「未公開の脆弱性」を突いて侵入し、「アップデート機能」が悪用されたとのことです。これを読み替えれば「企業が導入したセキュリティ対策基盤の脆弱性が侵入の糸口になり、さらに攻撃基盤として悪用された」と解釈できます。企業が信頼するセキュリティ基盤がゼロディ攻撃されると、不正アクセスの検知が難しいことも示されました。
第 7 位 （10 月）	**GoTo 利用し無断キャンセル千葉のホテル、被害 63 万円** コロナ禍における感染症対策や経済対策では、様々な政府施策がスピード感をもって導入された一方で、Go To トラベルや Go To イートの制度上の穴を突いて様々な不正が発生ました。また、あるいは事業実態のない者が個人事業主を装って申告して持続化給付金を不正受給したような問題も多発しました。
第 8 位 （6 月）	**期待の ISMAP 運用開始** 制度の目指す姿は、政府機関等で統一的なセキュリティ基準を明確化し、実効性・効率性のあるクラウドのセキュリティ評価制度を構築するものです。 5 月に ISMAP 運営委員会を設置、同月に第 1 回同委員会が開催されたことで運用が開始されました。10 月からクラウドサービスの登録申請が開始されており、審査に通ったサービスを登録した「ISMAP クラウドサービスリスト」（以下「ISMAP リスト」という。）が、2021 年 3 月には公開される予定です。
第 9 位 （11 月）	**カプコン、標的型ランサムウェアで最大 35 万人の個人情報流出か** ランサムウェアによる企業・組織への大きな攻撃がいくつかありました。 6 月には自動車メーカー・ホンダがランサムウェアによるサイバー攻撃を受け、世界的に業務の支障が出ただけではなく、海外の工場が停止したと報じられました。また、11 月にはゲーム大手カプコンから「ランサムウェア（身代金 ウイルス）による不正アクセス攻撃で、個人情報の流出が発生した」との発表がありました。
第 10 位 （11 月）	**経産相、IoT セキュリティ・セーフティ・フレームワークを策定** 経産省が IoT セキュリティ・セーフティ・フレームワーク（略称 IoT-SSF）を発表しました。IoT 機器が多様な特性をそなえ、さまざまなシステム構成や環境下で用いられることに配慮した、セキュリティ及びセーフティ対策のフレームワークです。IoT のセキュリティ対策はまだ始まったばかりで、今後も、利活用とセキュリティ対策を共に進めていく必要があると思われます。

４．お知らせ（トピックス）

業務研修の一環としてご好評を戴いている弊社の損保／生保公開講座をご案内します。

①日程

時期	損保講座基本コース	生保講座基本コース
2021 年 3 月	3 月 18 日（木）	3 月 17 日（水）
2021 年 4 月	4 月 22 日（木）	4 月 21 日（水）
2021 年 5 月	5 月 20 日（木）	5 月 19 日（水）

（注）新型コロナのため、現在は研修をリモート（ZOOM）形式で行っております。

②講座の内容

【損保講座基本コース】

- 受講対象者：損保関連業の未経験者から経験 3，4 年程度の方
- 講座内容
  －損害保険の概要（仕組み、損害保険会社の規模・組織など）
  －損害保険商品の種類、自動車保険、火災保険の仕組み
  ―保険契約の契約業務、保険販売(代理店）の詳細
  ―損保システムの概要、特色

【生保講座基本コース】

- 受講対象者：生保関連業の未経験者から経験 3，4 年程度の方
- 講座内容
  －生命保険の概要（仕組み、生命保険会社の規模・環境など）
  ―生命保険商品の種類、仕組み
  ―生命保険の業務
  ―生保システムの概要、特色

③申し込み方法

弊社ホームページよりエントリーをお願いします。

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　(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）