Ｐマークニュース

＜２０２２年爽秋号＞　Vol. ４１

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

カルチャーコンビニエンスクラブ(CCC)は、T カード利用者の個人データ販売を行うとし(2022.7.28 発表)、同意取得済の T 会員データ（T ポイントデータ）を、生活者のライフスタイルを基点とした情報プラットフォーム「CDP for LIFESTYLE Insights」として 8 月から提供を開始しました。使われるのは、全国５３００の提携企業から集めた私たちの利用履歴です。新たな形態の個人情報提供サービスですが、その「同意」をめぐって、議論があります。上記のサービスとこのサービスにおける改正法への対応と課題について、考察します。

連日のようにサイバー攻撃による被害が新聞等で報道されています。
警察庁では「令和４年上半期のサイバー空間をめぐる脅威の情勢等について」をこの 9 月に発表しました。サイバー攻撃の激化とその内容を如実に示す資料となっています。そこで本誌では警察庁の発表の中から
・被害を受けた企業規模に関する発生状況／「重大な脅威」なっているランサムウェアの脅威の実態／サイバー攻撃の感染経路／対策の実態に注目し、概要を解説しつつ、サイバー攻撃に対する注意喚起を行っています。

発生頻度を増すサイバー攻撃への対策は、各企業における経営課題のひとつといえます。このため各企業では様々な対処策（予防策）を講じつつあります。しかしながら、懸命な対処策にも拘わらず、サイバー攻撃を 100%防止することはほぼ不可能です。このため、被害に遭った際に、その被害を最小限に抑える方策を検討しておくことが重要になっています。

セキュリティインシデントの発生時のアクションフローの作成は、事後対策として有効性の高い方策です。このことからもセキュリティインシデント対策は、事前、事後両面からの対策が必要な時代を迎えていると言えます。

以上

１．本格化する個人データ販売　― 改正個人情報保護法の規定と必要な企業努力 －

カルチャーコンビニエンスクラブ(CCC)は、T カード利用者の個人データ販売を行うとし(2022.7.28 発表)、同意取得済の T 会員データ（T ポイントデータ）を、生活者のライフスタイルを基点とした情報プラットフォーム**「CDP for LIFESTYLE Insights」として 8 月から提供を開始しました。**使われるのは、全国５３００の提携企業から集めた私たちの利用履歴です。

新たな形態の個人情報提供サービスですが、その「同意」をめぐって、議論があります。

このサービスと、このサービスにおける改正法への**対応**と**課題**について、考察します。

（1）提供される「CDP for LIFESTYLE Insights」

「CDP for LIFESTYLE Insights」は、CCC マーケティング(株)とトレジャーデータ(株)が提供する情報プラットフォームです。CDP(Customer Data Platform 顧客データ基盤)は、**データを特定個人に紐づけるプラットフォーム**ですから、DMP(Data Management Platform)であり、外部から提供されるデータの活用基盤を「パブリック DMP」と分類すれば、いわば「プライベート DMP」とも言えます。

構成するデータは、「CCC マーケティング(株)の T サイト利用者データベース」と「トレジャーデータ(株)の契約企業の顧客データベース」です。

T サイト利用者データベースには、7,025 万人に関する個人情報があり(2022 年 3 月現在、名寄せし重複を排除して)、この会員が、いつ、どこで、何に、いくら使ったかの履歴を長期にわたり入手し、さらに機械学習でこれらの情報を一人一人プロファイリングし、「浪費タイプ」「助言信用タイプ」「肩書気にするタイプ」「情報拡散タイプ」など３７０以上の項目をスコア化したデータベース「顧客ＤＮＡ」が含まれていると言われています。ただ、CDP は、氏名や住所などは削除されて、提供されます。

トレジャーデータ(株)の顧客データベースには、同社と契約のある企業の顧客の氏名・住所・電話番号・メールアドレスをはじめ、スマートフォンの位置情報やアプリ利用データ、Web サイト・SNS 等でのユーザーの行動履歴やログ、さらには POS 等の販売データ、アンケートや各種リサーチデータ、もちろん IoT 機器から得られるデータ、DMP（パブリック DMP）が収集した外部データなども含まれていると思われます。

これらのデータベースを、メールアドレスと電話番号を識別子として、突合させ、そのデータを企業に提供します。CCC からは匿名加工された情報として提供されますが、受け取る企業は識別子によってどの顧客のデータか知ることができるので、「個人データの提供」に他なりません。

T ポイント利用者は、CCC や加盟店がデータを活用することは想定し、納得の上で使っているだろうが、ポイントと無関係の企業にまで情報が提供されると想像できるだろうか？

CCC 側は「利用規約で説明し同意をとっている」といいます。しかしながら、それは有効な「同意」といえるだろうか？

（2）グーグルの EU 個人情報規則違反への制裁

個人データの提供に関して想起されるのは、2019 年の EU の個人情報保護ルールの一般データ保護規則(GDPR)の違反として、フランス当局が米グーグルに 5 千万ユーロ(約 73.5 億円 10.22 レートで)の制裁金を命じた事例です。問題視されたポイントは２つありました。

第一は「個人情報の利用目的などをユーザーに明確に説明しなくてはならない」との規定への違反です。例えば、個人情報の利用目的などを説明したページが分散していてわかりにくい、位置情報の収集法を知るには、何度もクリックするなど 5 回から 6 回の操作が必要だったことなどです。

第二は、「ユーザーにきちんと同意をとらなくてはならない」との規定への違反です。

グーグルはアカウントを新規作成する際に一括して利用規約への同意をとっていますが、当局はターゲティング広告への活用など「同意は利用への目的別に、はっきりと行うべきだ」と強調し、グーグルの手法が不適切だったと判断されました。

この判断事例が 2020 改正個人情報保護法にどう反映され、CCC はどう対応しただろうか。

（3） [提供]に関する新たな改正法の規程

「個人情報の利用目的などをユーザーに明確に説明しなくてはならない」に関して、改正法では、次のように規定し、ガイドライン(通則編)で補足を加えています。

法第 15 条 (第1 項)

個人情報取扱事業者は、個人情報を取り扱うに当たっては、その利用の目的 (以下「利用目的」という。) をできる限り特定しなければならない。

ガイドラインの補足

利用目的の特定に当たっては、利用目的を単に抽象的、一般的に特定するのではなく、個人情報が個人情報取扱事業者において、最終的にどのような事業の用に供され、どのような目的で個人情報を利用されるのかが、本人にとって一般的かつ合理的に想定できる程度に具体的に特定することが望ましい。なお、あらかじめ、個人情報を第三者に提供することを想定している場合には、利用目的の特定に当たっては、その旨が明確に分かるよう特定しなければならない。

CCC の「CDP for LIFESTYLE Insights」ではどうだろうか？　この点に関しては、T 会員規約の「第 4 条：個人情報の取扱いについて」の「2. 個人情報の項目 3. 利用目的　」に詳細に記載されていますが、同意内容の記述に、下記で指摘する不安が残ります。

「ユーザーにきちんと同意をとらなくてはならない」に関しては、ガイドライン(通則編)で次の補足を加えています。

「本人の同意」とは、本人の個人情報が、個人情報取扱事業者によって示された取扱方法で取り扱われることを承諾する旨の当該本人の意思表示をいう（当該本人であることを確認できていることが前提となる。）

また、「本人の同意を得（る）」とは、本人の承諾する旨の意思表示を当該個人情報取扱事業者が認識することをいい、事業の性質及び個人情報の取扱状況に応じ、本人が同意に係る判断を行うた

めに**必要と考えられる合理的かつ適切な方法によらなければならない。**
なお、個人情報の取扱いに関して同意したことによって生ずる結果について、未成年者、成年被後見人、被保佐人及び被補助人が判断できる能力を有していないなどの場合は、親権者や法定代理人等から同意を得る必要がある。

CCC の「CDP for LIFESTYLE Insights」ではどうでしょうか？ T サイト［T ポイント/T カード］サービス利用規約の第 12 条-1 では、「（会員の個人情報を）行動ターゲティング広告事業者に第三者提供することがある」としており、広告事業者には「行動ターゲティング広告を自社の媒体で行う事業者」が含まれる、とあります。とすれば、広告が本業でなくても、顧客にダイレクトメールなどを送るほぼ全ての企業が対象になります。この規約を読んで、素直に、そう理解するのはむずかしいのではないでしょうか？法でいう「本人が同意に係る判断を行うために必要と考えられる合理的かつ適切な方法」とは言えなさそうです。

関連して、「個人関連情報の第三者提供の制限など」(法 31 条)が新設されています。
改正法では、[個人関連情報]を第三者に提供し、DMPなどを利用して、提供先で「個人データ」となる「提供」について、提供元での確認、提供先での当該本人同意(提供元での本人同意も容認)、提供元・提供先での記録の作成を規定している。

なお、「個人関連情報」とは、 生存する個人に関連する情報であって、個人情報、仮名加工情報及び匿名加工情報のいずれにも該当しないもの。例えば ①Cookie 等の端末識別子を通じて収集された、ある個人のウェブサイトの閲覧履歴 ②メールアドレスに結び付いた、ある個人の年齢・性別・家族構成等 ③ある個人の商品購買履歴・サービス利用履歴 ④ある個人の位置情報 ⑤ある個人の興味・関心を示す情報です。
従って個人情報に該当する場合は、個人関連情報に該当しません。
この規定により、CCCの「CDP for LIFESTYLE Insights」に本人同意の追加が必要になるでしょうか？ CCCが「CDP for LIFESTYLE Insights」を作成するにあたって、提供したTカード会員の個人情報は、「個人関連情報」に該当せず、新設された「個人関連情報の第三者提供の制限など」(法31条)は適用されないと思われます。提供する情報は、氏名や住所を削除して「匿名のままに保たれ、個人を特定できる情報は一切取得できない仕組みで提供される」(Tサイト［Tポイント/Tカード］サービス利用規約の第12条-4)ので、「匿名加工情報」として提供されていると思われます。(CCCのホームページには、「匿名加工情報」を取扱う旨が記載され、法定事項が掲載されています)「匿名加工情報」は「個人関連情報」ではないからです。従って、この法規制で、新たに「本人同意」を求めることは必要とされません。

規程改訂の有効性についての指摘があります。「該当部分の規約は、昨年 7 月の改定で追加された改定前からの利用者についても同意があるといえるのでしょうか？この改定の際、CCC側は登録者にメールで変更点を知らせたり、同意を取り直したりはしていません。

これに対し、名古屋大学の栗田昌裕教授（民法）は「規約を改定するだけでは個情法ガイドラインのいう『合理的かつ適切な方法』で『同意を得』たといえるか問題がある」と指摘します。民法では約款作成者に一方的な定型約款の変更を認めていますが、それは変更が合理的な場合や相手方の利益にかなう場合などに限られます。栗田教授は「第三者提供の相手先や提供情報の拡大は『合理的』ではないと判断され規約変更の効力が否定される可能性がある」とみる。」（読売新聞2022.9.3朝刊）

一方、ガイドラインにはこんな記述があります。（「個人関連情報」の項にではありますが）「本人の同意は、必ずしも第三者提供のたびに取得しなければならないものではなく、本人が予測できる範囲において、包括的に同意を取得することも可能である。なお、令和 2 年改正法の施行日前になされた本人の個人関連情報の取扱いに関する同意がある場合において、その同意が法第 26 条の2 第1 項の規定による個人関連情報の第三者への提供を認める旨の同意に相当するものであるときは、同項第 1 号の同意があったものとみなす（令和 2 年改正法附則第 5 条第1 号）」

（4）個人データ販売の本格化に向かって！

CCC の「CDP for LIFESTYLE Insights」販売について、CCC マーケティング(株)は「提供するレポートならびにT 会員のデモグラフィック情報などにより、企業は自社顧客のインサイトを深く理解することができ、市場環境の把握、製品やサービス開発、顧客一人ひとりのライフスタイルに応じたコミュニケーション等への活用により、さらなる顧客エンゲージメントの向上を図ることが可能です」としています。また、諸外国と比較して進んでいない日本のマーケティングを推し進めるものであり、「消費者である我々は企業のマーケティング活動に寛容になり見守る必要があるのではないか」という意見もあります。

これに対して、「自分の購買行動トレンド情報が第三者に提供されるのは気持ちが悪い」「約款に書いてあるから問題がないというのはおかしい。利用者に理解される努力をすべき」「こんな利用をされるのならT カード会員をすぐにやめたい。」などの投稿もあるようです。

個人データの利活用の推進は、2020 改正個人情報保護法改正の大きなテーマであり、**推進が必要です**。ただこのテーマは改正大綱で示された「保護と利用のバランス」「個人の権利利益を保護」が前提となるものです。保護のためには、「企業側は消費者を偽ったり、規約に記載した目的を超える範囲で利用者の情報を悪用することは絶対にあってはなりません」、加えて、そのチェック機構が有効に機能することが必要です。また、「個人の自由意思で「NO」と言える社会」が当たり前になり賛否を理解しあえる世情の醸成が必要と思われます。

「わたしのことを、知っている人がいる。わたしが好きなもの。わたしが嫌いなもの。それを知っている人がいる。それを思い出すだけですこし軽くなる。そう、世界はわたしが思うより温かい。あなたは、それを幸せと呼んだ。」（CCC マーケティング(株)HP「私たちのミッション」から）　と「個人の権利利益を保護」しつつ、「同意」の在り方などの現状課題をかかえながらも、一歩一歩、前進していくことを期待したいものです。**「消費者への正しい理解と納得」への一層の企業努力**が望まれます。

２．事例に学ぶ：警察庁「令和４年上半期のサイバー空間をめぐる脅威の情勢等」について

事例シリーズの第 17 弾です。先般恒例により JIPDEC から「2021 年度個人情報の取扱いにおける事故報告集計結果」(以下「JIPDEC 資料」)が公表されました。事故の原因(〝事象〟とした方がしっくりくるように思いますが)の NO.1 は相変わらず「メールの誤送信」です。

又、〝プライバシーマーク事業者の 6.2%の会社で事故を起こしており、事故を起こす事業者は複数回(約 3 回/年)発生させている〟の傾向も例年と大差はないように見受けられます。

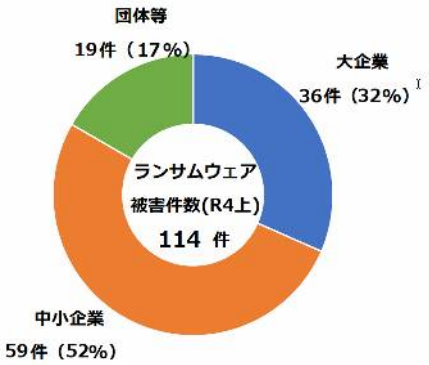
さて、今回は標題のように警察庁から 9 月に発表された報告書(以下「警察庁資料」)に基づいて考察してみようと思います。こちらは、当然ながら JIPDEC 資料よりも〝犯罪性〟に重きを置いた(メールの誤送信などは含まれない)分析となっているため、事案の母数は多くないものの重大性については吟味してみる価値があると考えます。

（１）被害を受けた組織の規模

警察庁資料では、「近年情報セキュリティに対する脅威が複雑・巧妙になり、被害先も著名な企業や機関に限らず地方の病院、**中小企業などに及んでいます**」などと解説されています。

例としてランサムウェアの被害（114 件）の内訳を企業・団体等の規模別にみると、大企業は 36 件、中小企業は 59 件であり、その規模を問わず、被害が発生しています。

【ランサムウェア被害の企業・団体等の規模別報告件数】



注）図中の割合は小数第１位以下を四捨五入しているため、総計が必ずしも 100 にならない。(以下同様)

勿論、企業の数(母集団)に対する比率では〝中小企業〟は微々たるものかもしれませんが、会社の存続に対するダメージは規模が小さい程大きいものになります。

2021 年の著名な事案に徳島県の病院の例があります。院内のサーバーで稼働する電子カルテシステムが利用できなくなりました。紙のカルテを作り上げるため 2 ヵ月を要し、その間本人に問合せしたり、調剤薬局から処方箋を取り寄せたりして患者の情報をかき集めましたが、会計システムなども連鎖的に利用できなくなり、診療報酬の算定や請求の業務が止まり、暫く収入を得られない状態での診療を余儀なくされたようです。**旧型の VPN 装置から侵入された**のが原因と報告されています。

（２）〝重大な〟脅威とは

警視庁資料では IPA の「2022 年十大脅威」と歩調を揃え、「ランサムウェア」にページの多くを割き最も重大な脅威と捉えています。理由は、ランサムウェアが暗号化した PC 等を復活させるための**キーを教えるための支払い(身代金)と併せて、窃取したファイルの流出・公開を抑えるための支払いも要求される**ようになっているからです。2021 年米国の石油関係の会社は数 100 億円の支払いを強いられたとの報道もありました。

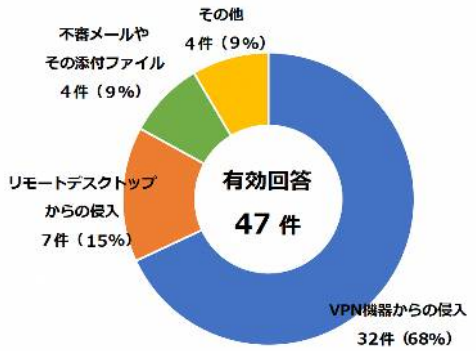
従って、ランサムウェア対策で**〝バックアップ〟が万全の策ではない**ことを意味しますが、バックアップはやはり必須です。バックアップにおいて、バックアップファイルが可視状態(自動同期や仮想ドライブ等)であればそのファイルも暗号化されかねません。バックアップが多世代を保管し、旧世代がエクスプローラで見えない(非可視)であれば侵害を受けることは防げます。バックアップシステムを選択する際の基準になります。

（４）で後述するように、暗号化されたファイルが 100%復元できるとは謳っていないものの、当該のファイルをアップロードして診断を受けられる国際的なサービスが出現していますので、一筋の光明と期待大です。窃取されたファイルが悪用されないようにするには、予めファイルを暗号化しておくしかないと考えます。

（３）攻撃の実態

ランサムウェアに限ったことではなく全てのマルウェアに通じることではありますが、警察庁資料ではランサムウェアの感染経路について分析されており、「VPN 機器からの侵入が 68%、リモートデスクトップからの侵入が 15%を占め」、テレワークにも利用される機器等の脆弱性や強度の弱い認証情報等を利用して侵入したと考えられるものが 83%」と大半を占めているようです。

【ランサムウェアの感染経路】



言い換えれば、ウィルス対策ソフト等の性能とユーザーの意識が向上し、旧来のテクニックでは攻撃しにくくなっているとも評価できます。

しかし、ルータに内蔵されているソフト(ファームウェア)の陳腐化や製造の終了に伴う脆弱性への対策は浸透していないと思われます。ルータだけではなく、ロボットソフトがいわゆる **IoT 機器やリモートデスクトップユーザを虱潰しにスキャン**しているとの報告が各方面から公表されています。

もう一つの話題に上っている「Emotet」についても、警察庁資料では「2021 年 11 月頃から活動を再開し、2022 年 2 月頃から再び被害が多くなった。(マイクロソフト Office や Zip ファイルに加え)**ショートカット(LNK)ファイルを用いた新たな感染手口**が発見された」としています。

（４）対策の実態

機器の脆弱性対策として、先ずは PC やサーバーにおいては OS 等を最新のものにアップデートする、パスワードを使い回さないなど、一般的なセキュリティ対策を確実に行うことが大前提です。

加えて、ルータの製造(購入)時期等も点検してみてはいかがでしょうか。例えば Elecom 社は、2017 年よりも前に製造された製品については〝アクセス可能な攻撃者によって、任意の

OS コマンドを実行される可能性があります〟と公表しています。しかも〝新しいファームウェアの提供はできない〟旨も買い換えるしかないと受け取れます。

更に、警察庁資料では組織として以下の点を強調しています。

✓テレワークの規程や運用ルールの整備

組織支給端末と私有端末の違いを考慮する。また、テレワーク開始時の暫定的な(緊急避難的)セキュリティ対策や例外措置とした運用を見直す。

✓従業員に対するセキュリティ教育の実施

家庭内ルータの点検と再設定を推進する。

✓利用するソフトウェアの脆弱性情報の収集と周知、対策状況の管理

欧州では、欧州刑事警察機構のサイバー犯罪対策機関である EC3(EUROPEAN CYBERCRIME CENTRE) がオランダ国家警察、McAfee と共同して、ランサムウェア対策のプロジェクト「**NO MORE RANSOM** 」を立ち上げ、ランサムウェアに関する被害ファイルの診断・復元サービス、復元ツールの提供等を行なっており、次の URL で復元ツールの利用法が解説されています。

https://www.nomoreransom.org/ja/index.html

併せて、**絶対送金しない**ようにと警告しています。身代金を払っても復元されず、再度攻撃される可能性(ランサムウェアが有効であることを攻撃者に証明することになります)があるからです。

（5）まとめ

個人情報に関する事故は、会社が本人に迷惑となる事象を主な対象としているのに対し、ランサムウェア被害のような情報セキュリティインシデントは主として外部から会社が攻撃を受ける事案を採り上げています。情報セキュリティインシデントは、個人情報保護の立場で言えば〝個人情報の滅失〟〝本人の同意を得ていない第三者提供〟(窃取された場合)に該当し、会社として個人情報の安全管理違反(極端な場合は法令違反)になります。

テレワークの常態化により社員の自宅作業環境が起因したインシデントであっても会社の責任は免れません。会社や自宅のルータを点検し、管理者パスワードを独自のものに代える等をされることが望まれます。ブラウザで(標準的には)「192.168.1.1」や「192.168.0.1」にアクセスしてルータのログイン画面を開き、管理者パスワードやパケットフィルタリング等の設定を見直しましょう。

３．セキュリティインシデントへの事後対応アクションフロー作成の勧め

最近は、企業や組織の情報漏えい事件や不正アクセス事件などの所謂「セキュリティインシデント」に関わるニュースが頻繁に取り上げられ、どのようにして「セキュリティインシデント」から企業を守るかは重要な経営課題になっています。そこで以下では、企業・組織が「セキュリティインシデント」対策を行う際のポイントを考えてみました。

（1）「セキュリティインシデント」について

「セキュリティインシデント」は、不正アクセス・サイバー攻撃による情報漏えいやウイルス感染パソコンや USB メモリなどの情報機器の紛失・盗難など、情報セキュリティに脅威を与える事象を指します。また、天災・人災による IT システムやネットワークの故障や損傷なども広い意味でのセキュリティインシデントに当たります。

ひと度セキュリティインシデントが発生してしまうと、①事実関係の調査に求められる費用負担（第三者機関への調査依頼コスト）、②被害顧客に対する損害賠償金や事後対応費用、③再発防止策として求められるセキュリティ環境の再構築コスト、④企業ブランドに対するイメージの低下、⑤顧客喪失による減収・減益、⑥企業ブランドに対するイメージの低下、、といった費用面での多額の出費や、企業の信用・イメージの悪化となります。

つまりセキュリティインシデントから企業が受けるダメージは大きく、企業・組織の存亡に関わる事態に繋がるおそれがあるのです。

従って、企業規模を問わず経営者は、明日にでも自社がこのようなセキュリティインシデントに見舞われる可能性があることを認識し、その対応を行うことが重要です。セキュリティインシデントへの対応策は、発生の防止策だけではなく、発生した場合に被害を最小限に留めるための対応策も併せ予め準備しておくことが必要です。

（2）セキュリティインシデント対策としてのアクションフローの作成について

サイバー攻撃の手口は日々進化しています。また、全く新しい手口のサイバー攻撃が生み出されたり、天災によってサーバーがダウンしたりするなどのインシデントもありうることを考えると、インシデントの発生を 100％防ぐことは不可能と言えます。

インシデントは、「事前の対策」によって発生を未然に防止することが一番ですが、事前策（発生防止策）とともに、インシデント発生時の事後対応として、アクションフローを予め策定しておくことが極めて大切になります。即ち、インシデント発生時のアクションフロー作成によって、以下のようなメリットを享受することが期待されます。

①セキュリティインシデントが発生したときに適切な対応をスムーズに取ることができる。

②情報セキュリティ担当者が迅速かつ効率的に復旧・処理にあたれるようになり、情報の漏えい規模、システムやサービスの中断などの影響を最小限に抑えられる。

③インシデント対応の際に得た知見を活用して、未知の脅威にも備えられるようになる。

事前の防止策を講じている企業は、最近増えつつありますが、不幸にしてセキュリティ

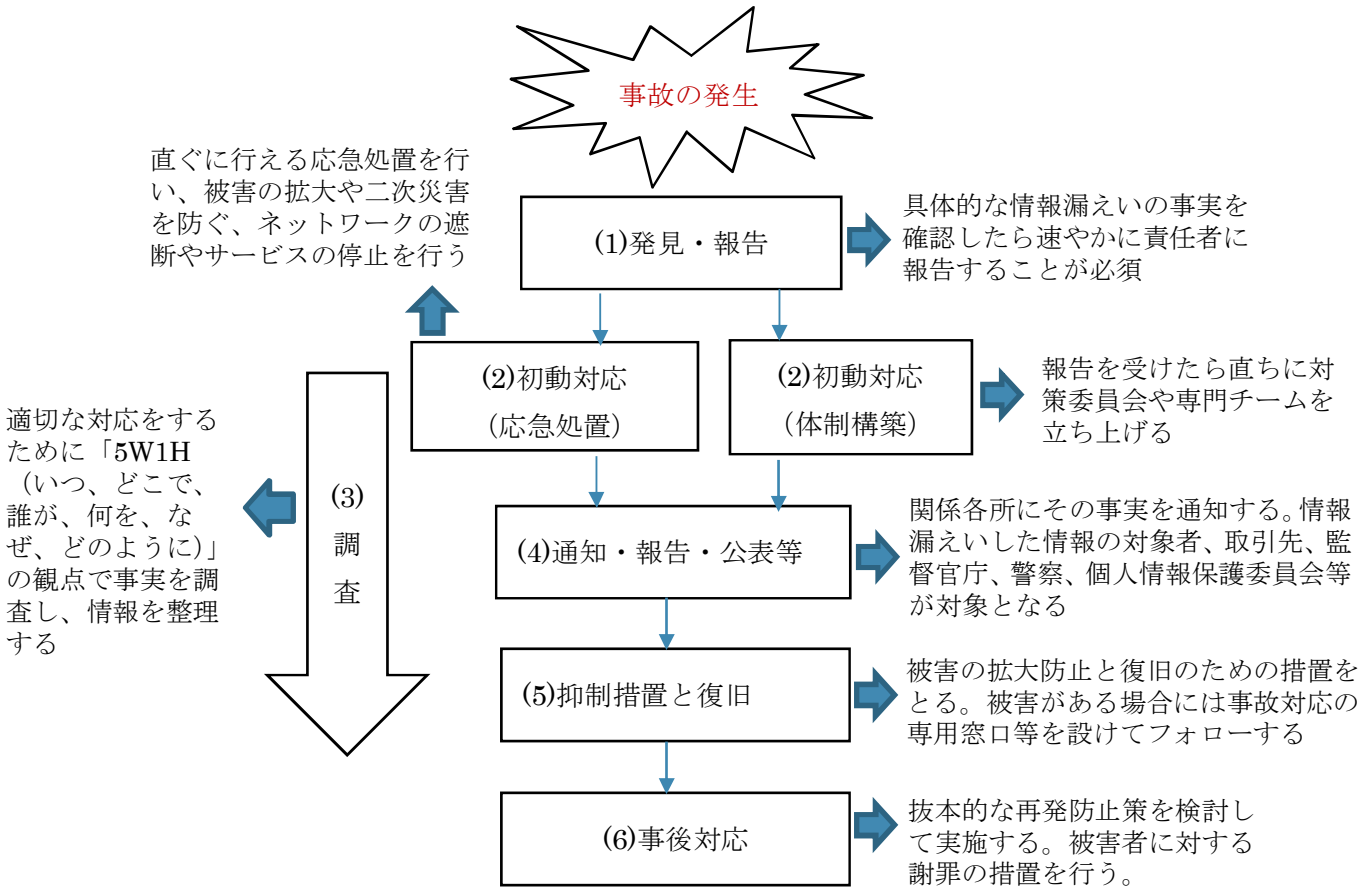
インシデントが起きてしまった場合に被害を最小限に留めるために「事後対応策」を用意している企業は稀だと思われます。しかしながら、昨今のインシデント状況は、事後策の策定をも促しています。

（３）アクションフロー作成のポイント

下図は、インシデント発生時のアクションフローです。そのアクション（行動）は６つのステップに分けられます。

各ステップにおける留意点を添えましたので、参考として下さい。

【ご参考：アクションフロー】



（４）最後に

今回セキュリティインシデントへの対応を本誌面で採り上げたのは、昨今、ランサムウェア等のサイバー攻撃による悲惨とも言える被害状況が伝えられているためです。おそらく被害を受けた企業の多くは「まさか当社が・・・」ではなかったかと思います。被害を最小化にするためには、「セキュリティインシデントが発生したらどうする？」といった問題を、普段から全社で共有し、社内の多くのメンバーを巻き込み組織的に対応策を策定しておくことだと思います。

さっそく御社に於いてもセキュリティインシデント発生時のアクションフロー作成にチャレンジしませんか？

４．お知らせ（トピックス）

（１）マイナンバーカードの交付率が５０％を超えました。

個人番号カード交付状況（2022 年 10 月 31 日現在／総務省）

区分	人口（R4.1.1 時点）	交付枚数（R4.10.31 時点）	交付枚数率
全国	125,927,902 人	64,384,833 枚	**５１．１％**

なお、全国レベルで 50%に達したのは 2022 年 10 月 19 日でした。

政府のマイナンバーカード普及への努力もあって、2022 年 10 月末現在のカード交付率は全国レベルで 51%（発行枚数約 5,000 万枚）になりました。これを年度比較すると 2020 年 10 月末 22%　⇒2021 年 10 月末 39%　⇒2022 年 10 月末 51%と推移しました。

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）