社労士と独立行政法人情報処理推進機構に聞く

SRPⅡ認証制度と SECURITY ACTIONの効果と活用

【前　編】

全国社会保険労務士会連合会（以下「連合会」という。）では、社労士の個人情報保護認証制度として、平成28年6月から「SRPⅡ認証制度」を開始している。一方、独立行政法人情報処理推進機構（以下「IPA」という。）でも、中小企業自らが情報セキュリティ対策に取り組むことを自己宣言する制度として、「SECURITY ACTION」を平成29年4月から始めた（各制度の概要は次頁参照）。

そこで今般、特別企画として、SRPⅡ認証を取得し、SECURITY ACTIONも宣言した社会保険労務士法人ミライエ代表の根本啓明氏と、IPA研究員の江島将和氏の対談を企画。両制度の活用方法やメリット、社労士の業務上必要な情報セキュリティ対策などについて意見を交わした模様を1月、2月号で前後編に分けてお伝えする。

※本誌24頁にSRPⅡ認証制度の申請方法のご案内を掲載しておりますので併せてご確認ください。

根本 啓明 氏

社会保険労務士法人ミライエ 代表社員

Profile

2008年6月、社会保険労務士登録。企業において16年間、人事労務系業務に従事し、社会保険事務手続、給与計算、福利厚生、人事給与制度設計、労働組合対応、人材育成、採用等、企業人事の全般に携わる。2013年4月、社会保険労務士法人ミライエ設立、代表社員。明治大学経営学研究科修了、修士（経営学）。

江島 将和 氏

独立行政法人情報処理推進機構（IPA）
セキュリティセンター　普及グループ研究員

Profile

外資系コンピュータウイルス対策メーカー、セキュリティコンサルティング会社を経て現在に至る。IPAでは、中小企業における情報セキュリティの調査、分析および研究業務に従事する傍ら、各種カンファレンス、セミナー等での講演や執筆活動を行う。情報処理安全確保支援士集合講習講師。大学院講師。中小企業診断士。

社労士全体で取り組む必要があると考えSECURITY ACTIONを宣言した

江島　IPAは、IT施策を技術面、人材面から支えるために設立された経済産業省所管の独立行政法人です。主に“情報セキュリティの確保”、“IT人材の育成”、“信頼性の高いシステムの開発促進”という３つの観点からその解決を目指し、“頼れるIT社会”の実現を目指しています。

なかでも中小企業の情報セキュリティに関しては、対策が十分ではないと感じている企業が約半数に上る調査結果も出ており、対策は急務です。IPAでは、「中小企業の情報セキュリティ対策ガイドライン」（以下、「ガイドライン」という。）の策定や「５分でできる！情報セキュリティ自社診断」（以下、「自社診断シート」という。）などのツールの開発、セミナーの開催などにより普及啓発を図っているほか、情報セキュリティに詳しい人材をセキュリティプレゼンターとして登録し、普及啓発に協力いただくなどの取り組みを進めています。

また、社労士会や商工会議所など、中小企業と関係の深い団体と連携した普及啓発活動も展開しています。平成29年２月には連合会の皆様を含めた中小企業関係団体と「中小企業における情報セキュリティの普及促進に関する共同宣言」を発表しました。さらに中小企業の自発的な取り組みを促すため、同年４月からSECURITY ACTIONという制度をスタートさせています。

根本氏が共同代表を務められている社会保険労務士法人ミライエさんでは、さっそくSECURITY ACTIONを宣言されていますが、まずはこの制度を宣言することになったきっかけを教えてください。

根本　『月刊社労士』平成29年３月号でSECURITY ACTIONの紹介記事があり、４月から始まる新しい制度だということで興味を持ちました。『月刊社労士』に掲載されるということは、すなわち連合会が社労士に推奨しているということですから、業界全体として取り組んでいくものであり、社労士の一人としてともに動いていく必要があると考えました。それがSECURITY ACTIONを宣言した理由です。

江島　SECURITY ACTIONのほか、SRPⅡやプライバシーマーク（以下、「Pマーク」という。）も取

SRPⅡ認証制度とSECURITIY ACTIONとは

●SRPⅡ認証制度

（社会保険労務士個人情報保護　事務所認証制度）

士業で唯一の個人情報保護の認証制度。社労士が顧問先の従業員等の個人情報を適正に取り扱っていることを認証し、「見える化」する。平成28年６月からマイナンバーや改正個人情報保護法施行に対応し、SRP認証制度からSRPⅡ認証制度へ刷新した。

●SECURITY ACTION

中小企業自らが情報セキュリティ対策に取り組むことを自己宣言する制度。取り組み目標に応じて２種類があり、「情報セキュリティ対策５か条」に取り組むと宣言することで一つ星のロゴマークを、「５分でできる！情報セキュリティ自社診断」で自社の対策状況を把握し、情報セキュリティポリシー（基本方針）を定めて外部に公開すると宣言することで二つ星のロゴマークを利用することができる。

得されていますが、取得されたのはいつ頃ですか。

根本　Pマークは平成27年10月です。マイナンバーが始まる前に何らかの対策を講じる必要があると考え、取得支援のコンサルティングには頼らず、自分たちで個人情報保護法を勉強して取得しました。かなり苦労しましたが、その勉強で身につけた知識の蓄積がありましたので、SRPⅡについては平成28年６月の制度開始早々に取得することができました。それまでもSRP自体は取得していて、まだ有効期限も残っていたのですが、企業側からSRPⅡを取得している社労士と、そうではない社労士が比較された場合は、やはりSRPⅡを持つ社労士が選ばれることになるので、早めに取得したいという思いがありました。

顧問先の従業員に安心感を与えるSRPⅡ 個人情報保護に取り組むアピールに

江島　それぞれの制度のすみ分け、あるいは違いについてはどのように考えていますか。

根本　対象が重なるところもありますが、違いも感じています。対外的に見ると、SECURITY ACTIONは個人情報に限らず企業に関する情報全般が対象ですが、Pマークは狭義の意味での個人情報を対象としています。一方で、SRPⅡは社労士の業務において、顧問先の従業員等の個人情報を適正に取り扱っていることの証しとなるものです。一見すると、SRPⅡはPマークと守備範囲が重なっているように思えるかもしれませんが、性質は違うと感じています。もちろん個人情報保護というベースは同じですが、SRPⅡは顧問先の従業員等の個人情報に焦点を当てていますから、社労士としてより明確なアピールになるものと理解しています。顧問先の従業員からすれば、自分の個人情報がミライエに預けられ、どのように取り扱われているか、不安に感じることもあると思います。そのような時に、社労士として個人情報保護にしっかり取り組んでいると説明する根拠になるものがSRPⅡであり、顧問先やその従業員に安心感を与えることができる制度だと思います。

江島　つまり、SECURITY ACTIONもSRPⅡも、さらにPマークも、それぞれ性質や対象に特徴があるので、それぞれ取得しておくべきだと考えられたわけですね。

根本　そうですね。たとえばPマークは個人情報の安全管理措置として組織的、物理的、人的、技術的といった４つの観点から対策に取り組んでおり、個人情報保護全般に関して適正に取り組んでいる法人だと、対外的に評価していただけるものと理解しています。ただ、すべての人がPマークの特徴を知っているわけではないので、詳しく知らない人にはその価値が十分に伝わらないかもしれません。その意味では、顧問先の従業員に対して認知してもらえるのは、やはりSRPⅡですし、SECURITY ACTIONという名称は、セキュリティというキーワードがあることで、セキュリティ対策に取り組んでいる企業であるということが知らない人でもイメージしやすいと思います。

また、ホームページにSRPⅡやSECURITY ACTION、Pマークなどのマークが表示されていれば、それだけで情報セキュリティにしっかり取り組んでいる社労士法人だというイメージを持っていただけるのではないでしょうか。口頭で説明しても伝わりにくいので、マークで視覚的に訴えたほうが効果は大きいと思います。それにマークがたくさんあると、単純にカッコイイという印象を持たれますし、ホームページの格も上がるように思います。

多額のコストをかけなくても 情報セキュリティ対策はできる

江島　SECURITY ACTIONは個人情報以外も保護対象としていますが、社労士の業務で、個人情報以外に情報セキュリティ対策の必要性を感じられたことはありますか。

根本　社労士は、顧問先の従業員等の個人情報を取り扱うほか、企業の経営・財務や事業計画等に関する社外秘の情報や、場合によっては投資家の行動に影響するような情報を知る機会もけっこうあります。もちろん社労士法上の守秘義務がありますので、外に漏らすことはありませんが、情報が漏えいするリスクはあるので、特にデータで情報をいただいた場合は規定に従って適正に管理や廃棄を行うなど、取り扱いには十分に気を使っています。

江島　個人情報以外にも顧問先の重要な情報を多く

取り扱うため、情報セキュリティ対策が必要ということですね。自社診断シートの項目にもある通り、重要な情報の保管や廃棄については、効果が高い情報セキュリティ対策の１つです。ミライエさんはSECURITY ACTIONの二つ星を申請されていますので、自社診断シートを実施されたと思いますが、いかがでしたか。

根本　基本的対策から従業員や組織の対策に関する事項まで、Pマークの取り組みと共通する点も多く、かなりクリアできていたと思います。

システム的な対策に関して言うと、多額のコストをかけて設備投資し、情報を守らなければならないようなイメージを持たれている人がいるかもしれませんが、決してそうではありません。たとえば私どもの取り組みを一つ紹介すると、メールの誤送信防止対策では、ミライエにはもうひとり共同代表（石上慶氏）がいますから、２人の机の間にモニターを置き、メール送信の際はそのモニターでメールの宛先等をお互いに確認してから送信するようにしています。時間的なコストは多少かかりますが、１分もかからない作業でセキュリティ効果があるので、設備投資にあまりコストのかけられない企業でも取り組みやすいのではないでしょうか。自分たちができる範囲と効果を考えながら、取り組むことが大切です。

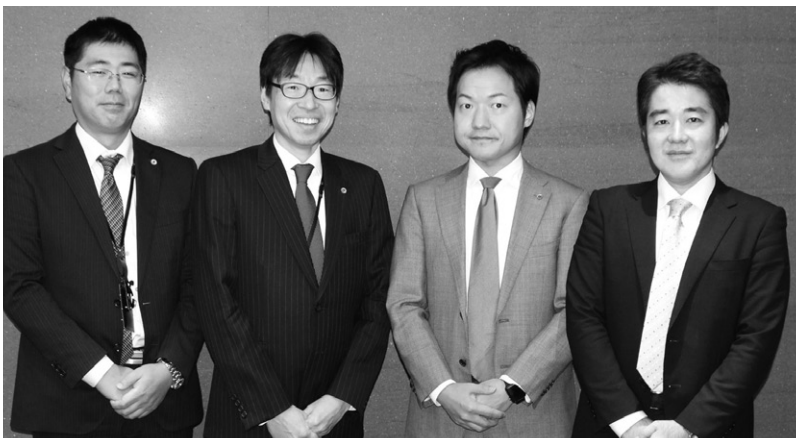
江島　ミライエさんの体制にあった対策を実施されているということですね。ガイドラインでは、経営者が認識すべき「３原則」として、業務の委託先に対しても同等かそれ以上の情報セキュリティ対策を求めるよう考慮する原則がありますが、それにはどう対処されていますか。

根本　顧問先の情報セキュリティ対策には、かなりの温度差がありますが、私たちは業務を委託される立場ですから、当然ながら一番高いレベルと同等かそれ以上のセキュリティを常に意識しています。

一方で、情報セキュリティにあまり意識が高くない顧問先に対しては、こちらからレベルを上げるようには言いにくいので、行動でセキュリティを高めるように誘導しています。たとえば顧客から個人情報のファイルにパスワードをつけないメールが送られてきた場合には、こちらから返信する時にパスワードをつけて送り返すようにすると、次回からは先方からもパスワードがついてくることはよくありますが、これだけのことで相手側のセキュリティレベルが少し上がるようになります。さらにファイルのやりとりをメールではなくクラウド上で行ったほうが容易ではないか、といった提案で、少しずつクラウドに移行を促していければ、設備投資もなく、ごく自然に相手側のセキュリティレベルを上げることができます。

江島　取引先を誘導することで、相互のセキュリティレベルの向上につなげているということですね。自社診断シートの対策内容はあまりコストをかけずにできることもありますから、根本さんのお話のように、情報セキュリティ対策の一つの対策基準として使っていただけるとありがたいと考えています。

（後編につづく）



対談には、社会保険労務士法人ミライエの共同代表である石上慶氏（左から1番目）と、IPAセキュリティセンター　普及グループの磯島裕樹氏（左から4番目）にも同席いただいた

社労士と独立行政法人情報処理推進機構に聞く

SRPⅡ認証制度と SECURITY ACTIONの効果と活用

【後　編】

対談には、社会保険労務士法人ミライエの共同代表である石上慶氏（左側手前）と、独立行政法人情報処理推進機構（IPA）の磯島裕樹氏（右側手前）にも同席いただいた

前編（本誌平成30年1月号）では、「SRPⅡ認証制度」と「SECURITY ACTION」の特徴と違い、社労士事務所内における情報セキュリティ対策の実践例について紹介した。

後編では、社労士業務としての情報セキュリティ対策、両制度を活用することのメリット等について、1月号に引き続き社会保険労務士法人ミライエ代表の根本啓明氏と、独立行政法人情報処理推進機構（IPA）の江島将和氏に伺う。

就業規則やテレワークへの対応など社労士のかかわりも多岐に広がる

江島　社労士として顧問先の情報セキュリティ対策の規定をつくるなど、業務としてかかわることはありますか。

根本　規定に関してはかなりあります。業務として作成するまではいかなくても、参考になるものがないかや、そこで規定された対策のレベルが適当かどうかご相談を受ける場合もあります。SRPⅡやプライバシーマーク（以下「Pマーク」という。）の取得によって、ある程度の知識はあるので、最低限保護すべきことや基準のレベルなどについてアドバイスできることはあります。

江島　就業規則の策定や改定の支援などでも、情報セキュリティ対策に関する対応が求められる場合がありますか。

根本　就業規則において求められるのは、機密保持に関する対応です。服務規律を設けたり、規定違反に対する懲戒規定を設けたりすることは、以前に比べて増えたと感じています。それから退職時の規定ですね。退職後の情報漏えいやノウハウ流出の防止に関しては、顧問先等からいろいろとご要望をいただきます。やはり情報漏えいの大部分は人為的なこ

とが要因ですから、どのようにリスクを回避するか、故意に漏らしている場合にどう対処するか、経営者の方が危機感を抱いているからだと思います。

ただ、会社が物理的にどんな対策を立てても、人が介在する限り、何かの情報漏えいが起こる可能性はあります。そうしたリスクを踏まえた対応が必要だと思います。

江島　人の問題も関係するだけに、難しい問題ですね。一方、近頃は働き方改革の関係で、テレワークのような多様な働き方がよく聞かれるようになりました。顧問先等からご相談を受けることもあると思います。これには働き方と同時に、情報セキュリティ対策もセットで考えていかなければいけない課題だと思いますが、そのあたりのお考えはいかがですか。

根本　企業が取り扱う情報によっては、テレワークに向き不向きがあると思います。つまり、外に出しても差し支えない情報を取り扱っているのであれば、テレワークに向いていると思いますし、出してはいけない情報があれば社内でやるほうが望ましいということです。それでもテレワークをやるというのであれば、別のセキュリティ対策を講じる必要が出てきます。その場合は、自宅で仕事をするのか、喫茶店のような公衆の場で仕事をするのか環境によっても対応が違ってきますし、パソコンを会社から持ち出すのか、持ち出して移動する間にどういったリスクがあるのか、一つひとつのリスクを考えて対策を明確にしておかなければいけません。おそらくそういった具体的なアドバイスが必要になると思います。

マイナンバーで高まる関心 それだけに効果が大きいSRPⅡ

江島　SRPⅡの取得やSECURITY ACTIONを宣言されたことで、具体的な成果が上がったり、業務に役に立ったりするなどのメリットを感じられたことはありますか。

根本　ミライエの場合、新規の取引が始まるのは、ほぼ100％ホームページが入口になりますので、そこにSRPⅡやSECURITY ACTION、Pマークなどのマーク表示があるのは、非常に効果があります。

SRPⅡ認証制度とSECURITY ACTIONとは

●SRPⅡ認証制度
（社会保険労務士個人情報保護事務所認証制度）

士業で唯一の個人情報保護の認証制度。社労士が顧問先の従業員等の個人情報を適正に取り扱っていることを認証し、「見える化」する。平成28年６月からマイナンバーや改正個人情報保護法施行に対応し、SRP認証制度からSRPⅡ認証制度へ刷新した。

●SECURITY ACTION

中小企業自らが情報セキュリティ対策に取り組むことを自己宣言する制度。取り組み目標に応じて２種類があり、「情報セキュリティ対策５か条」に取り組むと宣言することで一つ星のロゴマークを、「５分でできる！情報セキュリティ自社診断」で自社の対策状況を把握し、情報セキュリティポリシー（基本方針）を定めて外部に公開すると宣言することで二つ星のロゴマークを利用することができる。

情報セキュリティに対してしっかり取り組んでいる社労士法人だというアピールにもつながり、私どもをビジネスパートナーとして選定していただく大きな理由の一つになっているのではないかと考えています。現に、新規の顧客との打ち合わせにおいて、私たちがどのような情報セキュリティ対策を講じているのか、聞かれたことはほとんどありません。それというのは、マークが相手側に認知されており、先方の求めるレベルを十分にクリアしているからだと理解しています。そのような意味で、SRPⅡなどの認証制度は私どもの業務の拡充におおいに貢献していると感じています。

江島　平成27年10月にマイナンバー制度がスタートし、平成29年５月には改正個人情報保護法が施行され、個人情報の取り扱いがより厳格に求められるようになっています。企業における情報セキュリティに関する意識や考え方に変化を感じることはありますか。

根本　マイナンバーの導入によって、企業の意識はだいぶ変わったと思います。個人にマイナンバーが交付された時は、マイナンバーの対応だけにとどまらず、個人情報全般の規定をつくりたいというご相談が急増しました。個人情報保護に対する関心が高まったのは間違いないですね。

特に会社の経営者や人事担当者というよりも、従業員の意識が大きく変わったように感じます。メディアの影響もあると思いますが、たとえばマイナンバーを教えたくないだとか、マイナンバーが漏えいしたらどうなるのかだとか、個人情報の管理方法等に対する関心が非常に高くなりました。社労士は経営者や人事担当者とのやりとりが多いので、従業員から見ると自分たちの情報が社労士の事務所でどのように取り扱われて、何に使われているのかが見えにくく、ブラックボックスになりがちです。しかし、そこでSRPⅡを取得していれば、少なくとも個人情報はしっかり取り扱ってくれるだろうと思ってもらえます。その効果は大きいと思いますね。

一方で、個人情報保護法改正は驚くほど反応がないので、少し心配しています。特に中小企業にとっては、そこで初めて法の適用対象になるというところも多いように思うのですが、今のところ大きな変化は感じられません。個人情報保護法への取り組みが遅れているのかもしれませんので、顧問先等には注意を促しています。

根本 啓明 氏

社会保険労務士法人ミライエ 代表社員

江島 将和 氏

独立行政法人情報処理推進機構（IPA）
セキュリティセンター　普及グループ研究員

人を大切にするための情報セキュリティ対策が不十分な企業に人は集まらない

江島　情報セキュリティ対策に取り組むことは、社労士としての武器になるとお考えですか。

根本　間違いなく武器になると思います。社労士は労働社会保険や労務管理の専門家ですが、顧問先等からご相談を受けるのは、専門分野に限ったことではありません。相談内容によっては他士業の管轄になりますが、個人情報保護や情報セキュリティに関

しては、それが知識としてあれば個人情報保護規程や就業規則におけるアドバイスのみならず、さらに相談の幅も広がります。また連合会は制度創設50周年を迎えるにあたり、「人を大切にする企業」づくりの支援をスローガンに掲げていますが、個人情報の漏えいを防ぐことは、まさに人を大切にすることにつながるものと捉えています。

江島　昨今は人手不足ですから、情報セキュリティがしっかりしていない企業だとわかれば、いい人材が集まらないということも考えられますね。

根本　そうですね。就職活動も転職も、履歴書という形で自分や家族の個人情報を企業に提供するわけですから、提供先が増えれば増えるほど、個人情報漏えいのリスクが高まります。個人情報の管理や廃棄の規定がきちんとあって、そのとおりに運用している企業は、基本的には問題ないと思うのですが、そうではない企業も多くある中で、自分の個人情報を提供することに危険を感じさせるような企業には、当然ながら人は集まりません。さらに言えば、情報漏えいがあった企業は、情報セキュリティ対策が緩いと思われるだけでなく、それ以外の対策についても緩いと思われます。企業の信頼性にもかかわる重要な問題です。

江島　その意味では、社労士の皆様もSRPⅡやSECURITY ACTIONといった制度を活用し、情報セキュリティ対策にしっかり取り組むことが今後ますます重要になってくるということでしょうか。

根本　そうだと思います。もちろんSRPⅡの取得やSECURITY ACTIONを宣言することは重要ですが、大事なことは制度ありきではなく、情報セキュリティの重要性を認識し、対策にしっかり取り組むことです。業務の執行体制や情報の取り扱い、それに要する時間やコストなどを把握し、現時点でできないことをリスクとして認識し、将来に向けて改善方法を検討していくことができれば、おのずとSRPⅡを取得し、SECURITY ACTIONを宣言できるはずです。業務の現状把握などに時間はかかるかもしれませんが、ハードルは決して高くありません。情報セキュリティは今後ますます重要になりますし、いずれはすべての社労士がSRPⅡを取得するくらいのレベルにならないといけないと考えています。

江島　本日は貴重なお話をいただきました。ありがとうございました。

（おわり）