参考資料2

関係者限り

2019年度　第2回 中小企業の情報セキュリティ普及推進協議会　議事メモ

日　時：2019/8/7(水)　15:30～17:00
場　所：IPA 15階 委員会室2,3
出席者：(団体名50音順)

(一社)中小企業診断協会	専務理事	野口 氏
全国社会保険労務士会連合会	業務部長	福岡 氏
全国商工会連合会	会員サービス課長	起田 氏
全国中小企業団体中央会		ご欠席
(特非)日本ネットワークセキュリティ協会	理事	下村 氏
(特非)ITコーディネータ協会	研修制度ﾃﾞｻﾞｲﾝ部　参与	松下 氏
(独)情報処理推進機構	ｾｷｭﾘﾃｨｾﾝﾀｰ長	瓜生
(独)中小企業基盤整備機構	経営支援部長	中島 氏
日本商工会議所	情報化推進部　課長	岡本 氏
日本税理士会連合会		ご欠席
[ｵﾌﾞｻﾞｰﾊﾞ]　経済産業省　商務情報政策局　ｻｲﾊﾞｰｾｷｭﾘﾃｨ課　課長補佐		西野 氏
経済産業省　商務情報政策局　ｻｲﾊﾞｰｾｷｭﾘﾃｨ課　係長		野村 氏
中小企業庁　技術・経営革新課　課長補佐		小池 氏
中小企業庁　技術・経営革新課　係長		丹 氏
IPA事務局		横山、近藤他

議　事：　※網掛け部分は宿題事項

1．開会
- 配布資料の確認、オブザーバ紹介［IPA近藤］

2．2019年度活動状況　＜資料1＞
- 資料1の説明［IPA磯島］
  協議会としての活動状況として、SECURITY ACTION制度の普及への取り組み、中小企業等への直接的な働きかけの状況を報告。

3．「全国中小企業クラウド実践大賞」の開催について
- 資料2-1の説明［日本商工会議所　岡本氏］
  中小企業のクラウド活用を進めるためには取り組みの見える化が必要であると考え、SECURITY ACTION制度を参考にした自己宣言および表彰の取り組みについて、CLOUDILを事務局とした実行委員会形式で開催する「全国中小企業クラウド実践大賞」の紹介。

岡本氏：総務省・経済産業省がキャッシュレス実証実験を実施している地域を中心に地方大会を5会場で実施する。その中の優秀事例にて、12月～年明けに全国大会を開催予定。自己宣言およびコンテストへの参加企業を増やしていきたいため、皆様のご協力をお願いする。

中島氏、：地方大会5会場のいずれかに出ないと全国大会には出れないと考えて良いか。

岡本氏：その通り。所在地にかかわらず、どの会場へも応募可能だが、プレゼンを行うため近い会場が便利

だと考える。

野口氏 ：中小機構も後援を出す予定と聞いており、中小企業診断協会、ITコーディネータ協会なども後援に入る予定。

4．全国横断サイバーセキュリティセミナー2019

➢ 資料3の説明［JNSA下村氏］

9月～11月に開催するセミナーの内容紹介と集客の依頼を実施。

下村氏 ：講演者にISOG-Jとあるが、これはJNSA配下のセキュリティオペレーション事業者の協議会であり、脆弱性検査の方法など検討している。JNSAツールの紹介については、昨年公開した「CISOハンドブック」の中小企業版を作成しており、完成予定のため、その紹介を中心に実施する予定。集客に関して皆様のご協力をお願いする。

5．2019年度IPA中小企業への情報セキュリティ対策普及事業

➢ 資料3の説明［IPA横山］

IPAの取り組みとして、H30補正事業の3事業の取り組み状況と協力依頼、従来事業の取り組み状況の報告を実施。

IPA横山：「宮城県・岩手県・福島県」「長野県・群馬県・栃木県・茨城県」「石川県」「広島県」の4地域が実証に参加する中小企業の集客に苦戦しているため、この地域への働きかけのご協力をお願いする。

IPA近藤：本日「中小企業の情報セキュリティマネジメント指導業務」に関するメルマガ周知文案を各団体へ送付しているため、周知の協力をお願いする。

中島氏 ：お助け隊の東北の事業説明会が仙台となっており、宮城県・岩手県・福島県が1つの実施地域となっているが、仙台と盛岡は180km離れていて東京－静岡と同じ距離であり、この3地域が同じ場所に集まることはまずない。仙台で実施したとして電車・車で1時間程度の石巻からでもなかなか来てもらえないのが東北の実状。参加事業者を集めるためには、もう少しきめ細かい戦略を立てると効果が出るのではないか。

IPA近藤：経済産業省の方が東北地域を訪問して主力企業と意見交換した際にも、東北地域を一括りにしてしまうと人集めが難しいとの指摘をいただいているため、実施者に対して指導を徹底したい。

野口氏 ：「中小企業の情報セキュリティマネジメント指導業務」の登録セキスペに対する謝金はどの程度か。

IPA近藤：交通費込みで45,000円/回で1社4回までの支援を予定している。近隣の専門家を紹介する形式で東京から交通費をかけて地方に行くようなことがないように工夫する。

野口氏 ：実施者は地元の支援機関にはどの程度アクセスしているか。福島県ではよろず支援拠点を中心に中小企業支援ネットワークができており、県内すべての支援機関とつながっている。広島県の場合は地域の金融機関が中小企業のIT支援に積極的である。こういった機関に声がかかっていなければ協力を依頼すると良い。中小企業診断協会も中小企業診断士だけでは活動範囲が限られるので、地域金融機関と連携する戦略をとっている。石川についてはすぐには思いつかないが、広島は広島銀行などが積極的である。

IPA横山：石川については富山、福井などへの対象地域の拡大も検討している。

野口氏 ：北陸は北國銀行が中小企業支援に力を入れていると聞いている。

IPA近藤：お助け隊の実施者は、地元の支援機関に対してローラーで働きかけているが、ご指摘いただいたような地域で有力な支援機関に対して漏れがないか確認しつつ、もうワンプッシュかけることを検

討したい。また、地場の有力企業（大企業、金融機関、インフラ事業者など）への協力依頼も並行して実施している状況。

松下氏 ：「中小企業の情報セキュリティマネジメント指導業務」の目的は、中小企業の実態を把握してどういう支援をすれば良いか、また地域のネットワークを作って継続的な支援を実施する人材を地元に定着させるなどが考えられるが、適切なプロフィールの人がアサインされて定着できるような事業になっているのかを知りたい。

IPA 近藤：実証事業の目的としてはご認識の通りであり、アサインされる方の適性などは重視する必要があるが、今回は実証事業のため、事業説明会に参加した登録セキスペで中小企業支援に意欲がある方であれば、まずはトライしてもらう方向で考えている。中小企業 400 社に対して登録セキスペも相応の人数が参加する見込みのため、指導事例など集まった結果の分析を通じて人材面に関する考察なども行いたいと考えている。

松下氏 ：4 回で終わりなので「あとは勝手にやってください」とならないようにしないといけない。

IPA 近藤：次に繋がる考察・分析結果となるように事業を進めていく。

下村氏 ：4 回以上はオプションで実施しても問題ないか。

IPA 横山：事業としては 4 回まで支援する。うまくいくようであれば、その後は双方の合意次第で個別に有料で継続してもらうことは問題ない。

野口氏 ：登録セキスペの属性として、例えば独立してコンサルをしている方がどれくらいいるかなどは把握しているか。

IPA 近藤：IPA 国家試験部で保有しているデータと、登録セキスペ向けに実施している調査の結果もあるため、所属の属性や得意な領域などの情報はある。

下村氏 ：実証結果としてばらつきが大きく出ると思うが、指導事例に関しての評価は実施予定か。

IPA 横山：実施する。特にうまくいかなかった事例はしっかり評価をしていく予定で、場合によっては訪問調査も考えている。

下村氏 ：「中小企業のサイバーセキュリティ製品・サービスに関する情報提供プラットフォーム構築に向けた実現可能性調査」にサービスが含まれているようだが、情報セキュリティサービス基準の適合審査との関係はどうなっているか。

IPA 横山：サービスを入れているのは、製品とサービスを一体で提供しているケースを考慮して幅広く対象としている。今回は実現可能性の調査なので、製品・サービス部分も含めて整理していく。

下村氏 ：例えば「脆弱性検査サービス」で今回の事業で調査して良いサービスだという結果が得られて、「情報セキュリティサービス基準適合サービスリスト」には登録されていない場合どうなるのか。

IPA 瓜生：製品・サービスとあるが、実際は製品がメインで、サービスについては製品に紐づくサービスの意味合い。イメージとしては製品版のぐるなびのようなもの。「情報セキュリティサービス基準適合サービスリスト」に登録されているサービスについても評価はどうなのかといった議論になった場合には影響があるかもしれない。

下村氏 ：「製品・サービス」の表現は製品とサービスが別物ではなく、製品とその製品の運用サービスという理解で問題ないか。

IPA 瓜生：その通りである。ベンチャーが提供している製品・サービスでも良いものがあるため、それらを発掘しようという目的。

下村氏 ：どちらも IPA が提供するものなので、ユーザーが混乱しないようにしないといけない。

IPA 瓜生：毎年審査して登録しているが、登録事業者のサービス自体を評価することは実現できるものか。

下村氏 ：サービス内容の審査まではできないから事業者としての登録審査となっている認識。今回の事業では検証を実施するということで、より踏み込んだものでチャレンジャブルな取り組みと考える。

IPA 横山：今回はあくまで実現可能性の調査であり、その中でどこまでできるかについても確認していく。

IPA 近藤：先日の産業サイバーセキュリティ研究会 WG3 でも同様の質問があり、その際に経済産業省サイバーセキュリティ課から説明があった内容としては、サービス事業者の最低限の担保をするのが審査登録制度の目的で、今回の事業は製品そのものを中小企業目線で判断できるように情報提供することが目標で、相互にリンクを貼ることは選択肢としてあるが、別物として整理していくという考えであった。

野口氏 ：補正事業での実施だが、成果物のメンテナンスは継続される予定か。

IPA 近藤：実施主体も含めて、今回の実現可能性の調査の中で並行して検討していく必要があると考えている。必ずしも IPA が継続して実施することを前提とはしていない。

6．SECURITY ACTION 三つ星(仮)検討

➢ 資料 4 の説明［IPA 田居］

SECURITY ACTION 二つ星の次の段階の取り組みとして三つ星の検討に関する経過報告を実施。

下村氏 ：中小企業の情報セキュリティ対策ガイドライン記載のリスク分析を実施するのはハードルが高いか。

IPA 田居：ガイドラインを第 3 版に改訂するにあたり、リスク分析の扱いを変えた経緯もあり、ハードルは高いと考える。

下村氏 ：さらに取り組んでほしい部分としてリスク分析などを 3 段階目とする考え方ではないか。

IPA 田居：感覚的ではあるが、現時点ではそれは四つ星レベル。

野口氏 ：この基準では政府調達の要件には入らない。良くて加点要素だろう。政府調達に入れるのであれば、経済産業省と相談が必要であり、総務省の政府調達の基本方針などとの検証も必要と考える。

IPA 瓜生：中小企業であれば、または C・D ランクであれば、このレベルで良いなどの考え方はないか。

野口氏 ：中小企業や C・D ランクであればといった考え方は難しい。事業の性質上セキュリティの扱いが軽いものなら良いかもしれないが、扱いが軽いものに対して義務化ができるかが問題。加点要素と義務(要件)とは重さが違う。過去に、政府調達の要件に情報処理技術者試験合格者に並べて IT コーディネータ試験合格者を入れようとした際も苦労した。IPA が認証したという形であれば変わってくるかもしれないが、レベルが高くなり費用もかかることになり利用してもらえなくなる可能性がある。一方で民間調達のニーズがどの程度あるかが明確になって、制度として普及していけば国も受け入れやすくなるかもしれない。

下村氏 ：P. 6 の図に違和感があり、NIST SP-800 は大企業だけでなく、小企業も対象ではないか。あえて記載するのであれば小企業の技術対策の領域まで円を伸ばすべき。PCIDSS もそうだが規模の大小は関係ない。小企業の技術よりの空白部分だが、あるとすれば国の統一基準などであり、これも大小は関係ない。SECURITY ACTION 三つ星に関してはマネジメントシステムを持っていることを第三者が確認するレベルだろう。出口部分でどれだけ調達要件にできるかが問題だが、これからは事業分野に依存するような、もっと個別の要件が出てくる。「技術等情報の管理に係る認証制度」などは信用が出てくることが予想され、この制度は分野ごとになっていくだろう。ただし分野ごとになったとしてもベースは必要であり、セキュリティマネジメントシステムがない上にいくら基準を作ってもすぐに劣化する。そのベースという位置づけであれば SECURITY ACTION 三つ星は合うと考える。

下村氏 ：P. 4 情報通信業の「すべてのレイヤーで同一の基準を要求することも難しい」とあるが、同一基準とせざるを得ない時代になっているため、この意見に引きずられるのは良くない。三つ星の事業者に対策を要求したら、それを実装して回してくれる信頼できる企業であるという位置づけであり、

関係者限り

三つ星を信頼するのではなく、しっかり対策事項を伝える必要がある。

IPA 田居：契約などで明確にし、単に要求に対して「やります」というだけではない体制を構築することが必要だという認識でいる。

下村氏 ：P. 10 記載の情報セキュリティ内部監査人 (JASA) は人数非公開だが、情報セキュリティ監査人 (監査人補含む) は公開されており 1,000 人を超えている。

中島氏 ：個人的な見解だが、今回の三つ星は少しロジックが変わっており、受け手のことを考えると IPA が認証するのであれば SECURITY ACTION とは別物にすべき。手間をかけないのであれば、5 年間継続などの実績を積み上げていったら三つ星になるのが分かりやすくて良いのではないか。そういう意味では P. 14 の方向性は良いと考える。

松下氏 ：三つ星を作るのであれば取得のメリットをはっきりして欲しい。メリットとは、政府調達の要件になるか、大企業のサプライチェーンに入るための資格になるかが分かりやすい基準と考える。使う側からみると信頼性の確保が重要であり、それは既存の政府調達の要件や大企業の調達条件から紐解くしかなく、それをどこまでミニマムにできるか。最後に運用可能な費用がどの程度かが問題であり、P. 12 に「10 万円以下」の記載があるが、これは非常に現実的な価格だと考えるが、これで制度が回るような設計が必要になる。信頼に値するものを作り上げることがもっとも大変である。すでにそういった制度を運用している JIPDEC などの機関ともうまく連携して確認していきながら、しっかり実現できる範囲で進めてほしい。

野口氏 ：P. 15 にスケジュールがあるが、良い制度を作るためには時間がかかっても仕方がないので、このスケジュールにこだわる必要はないと考える。

IPA 瓜生：IPA の中期計画の目標を自己宣言者数ではなく、ステップアップ数に切り替えた。中小企業の行動を促すために二つ星の次の取り組みは必要と考え、制度は検討していく。

7．閉会

野口氏 ：「中小企業の情報セキュリティ対策ガイドライン」の普及に協力できないかと考え、今年の中小企業診断士試験の問題にガイドラインに関連する問題を入れたことを報告する。

IPA 瓜生：今回の主目的は三つ星の議論であり、IPA の計画としては当初 5 年間で 25,000 件を目標としていたが、皆様のご協力もあり既に達成し、次のステップとしては数を追うのではなく質の向上を目指していきたい。クラウドサービスの安全性評価の検討会なども行われているが、何かしらのサービスに対する評価を実施して安心できるものを使っていくということは、全世界的に求められていると感じるので、そういったものをどうやって実現していくかがこれからのセキュリティの課題だと考えるため、現場をよくご存じの皆様のお力添えをいただきながら取り組みを進めていきたい。

IPA 近藤：次回は 10 月下旬から 11 月上旬での開催を予定。あらためて別途メーリングリストにてスケジュールを確認させていただき、日程を確定する。

以上