資料２－２

中小・小規模事業者の情報セキュリティ対策の強化に向けた意見【骨子】

■基本的な考え方

・事業活動を行う上で、インターネットの利用は不可欠。『「日本再興戦略」改訂２０１５』の中の施策の一つとしてＩｏＴの活用が取上げられるなど、ビジネスの現場においてＩＣＴの利活用は今後更に重要となる。
・サイバー犯罪の件数は年々増加傾向。手法も高度化している事から脅威は増大。ＩＣＴの利活用はサイバー空間を安全・安心に利用できてこそ成立するものであり、情報セキュリティ対策と車の両輪で進める必要がある。
・中小・小規模事業者は大企業と比較し、情報セキュリティ対策に関する取組みを行っている割合が低い。個人情報保護法の改正やマイナンバー制度の開始に伴い、全ての企業に情報セキュリティ対策が求められる中、経営者の意識改革を中心にこのような状況は改善が必要。

■意見項目

１．情報セキュリティ対策の意識向上・強化
①経営者の情報セキュリティ対策に関する意識の向上・強化
②ＢＣＰ（Business Continuity Plan）への取込み
③中小・小規模事業者も活用できる「サイバーセキュリティ経営ガイドライン」の解説などの策定
④情報セキュリティ対策に対する啓発
⑤中小・小規模事業者支援機関の取組み支援

２．情報共有・連携の強化
〇被害後の情報共有及び官民の情報連携の強化

３．相談体制の周知ならびに拡充
①ＩＰＡ（独立行政法人情報処理推進機構）相談窓口の積極的なＰＲ及び相談体制の拡充
② 対面型による相談窓口の設置及び拠点化

４．情報セキュリティ人材の確保・育成
①中小・小規模事業者が情報システム担当者を雇用する際の支援
②人材の供給支援
③人材育成の環境整備
④新設される「情報セキュリティマネジメント試験」の普及・啓発
⑤新設される「情報処理安全確保支援士」の普及及び活用促進

５．情報セキュリティ対策に必要な設備導入の促進
〇中小・小規模事業者が情報セキュリティ対策ソフト及び設備機器を導入する際の

支援

６．被害拡大防止の支援

〇被害後に行うデジタルフォレンジック（データの保全・復元・解析）に対する支援

７．国際イベント・法改正等に対する取組み

①２０２０年東京オリンピック・パラリンピックへの対応

②マイナンバー制度、改正個人情報保護法（５０００件要件撤廃）への対応

③中小・小規模事業者が保有する知的財産保護への対応

以　上

中小・小規模事業者の情報セキュリティ対策の強化に向けた意見

２０１６年4月１４日
東 京 商 工 会 議 所

はじめに

ＩＣＴ（Information and Communications Technology）の進歩はビジネスに大きな変革をもたらした。時間や場所にとらわれず経済活動を行うことが可能となり、また、人と人に限らず、モノとモノ、さらに人とモノとがつながることも容易にした。ＩｏＴ（Internet of Things）はその代表的な例である。モノがインターネットとつながることにより、計測したデータの送信や遠隔地からコントロール、最適な状態を維持することが可能となり、上手く活用できれば生産性の向上につながる。例として、水田にセンサを設置し、湿度・温度・水位・水温などを自動で計測・解析を行うことで収穫量増加・品質向上に成功した事例は、まさにＩＣＴの賜と言えよう。今後、様々な分野での新たなイノベーションが創造され、日本経済の成長において無限の可能性を秘めていると言っても過言ではない。

一方、ＩＣＴを利活用することは、個人情報や企業情報などの多くのデータを持つことになる。情報を保有する上で、情報が漏えいしないように情報セキュリティ対策を行うことは、ＩＣＴを利活用する上で必要不可欠である。つまり、ＩＣＴの利活用と、情報セキュリティ対策は車の両輪の関係にあると言える。

サイバー攻撃の件数は年々増加し、手法も巧妙かつ多様化しており、個々の事業者が、情報セキュリティ対策を行うことは必須事項である。しかし、対策を行うにも社内に情報システム担当者がいない、情報セキュリティ対策の費用が捻出できないなどの課題がある。とりわけ、中小・小規模事業者においては、情報セキュリティ対策が大企業と比較すると遅れている実態がある。中小・小規模事業者は、マイナンバー制度や個人情報保護法及び不正競争防止法の改正などの影響もある事から、このような事態は早急に改善しなければならない。

こうした状況を踏まえ、中小・小規模事業者に対する情報セキュリティ対策を推進すべく、以下の通り意見をとりまとめた。

Ⅰ．基本的な考え方（現状と課題）

①ＩＣＴ利活用を取り巻く現状

ビジネスの現場において、インターネットの利活用の機会は益々増えている。総務省の「通信利用動向調査」によると、２０１４年度末の企業におけるインターネット普及率は９９．６％に達しており、事業活動を行う上でインターネットの利用は必要不可欠である。また、２０１５年６月３０日に閣議決定された『「日本再興戦略」改訂２０１５』の中の施策の一つとしてＩｏＴの活用が取上げられるなど、ビジネスの現場においてインターネットを利用したＩＣＴの利活用は今後更に重要となる。

②情報セキュリティへの脅威の現状

ＩＣＴの利活用はサイバー空間を安全・安心に利用できてこそ成立するものであり、情報セキュリティ対策と車の両輪で進める必要がある。

昨今、サイバー犯罪の件数は年々増加傾向にあり※注－１、手法も高度化していることから脅威は急速に増大している。また、一口に情報セキュリティの脅威と言っても外部からの攻撃のみならず内部要因など様々な要因がある。

【外部要因】

・マルウェア…コンピュータウィルスやスパイウェアなどの不正かつ有害な動作を行う意図で作成された悪意のあるソフトウェア。最近では、ランサムウェアなどがある
・不正アクセス…ホームページの改ざん、乗っ取り、なりすまし。近年ではWebサイトを改ざんし、アクセスした利用者にウィルスなどの仕込む水飲み場型攻撃などがある
・サービス不能…アンプ攻撃（大量のデータを一斉に送信して対象のサーバーに多大な負荷を与え、サーバーをダウンさせる）

【内部要因】

・宛先の選択ミスや添付ファイルの取り違えなどのメールの誤送信
・出先での個人情報などの置き忘れ、盗難
・従業員または委託先の会社の従業員の意図的・過失による情報の流出
・ＳＮＳ炎上、ヒューマンエラー
・誤操作によるデータの喪失

※注－１：警視庁の発表によると都内のサイバー犯罪の検挙数は２０１０年において６３１件だったのに対し、２０１４年は1，１８０件とほぼ倍増している。２０１５年は１０月時点では９０１件。

上記以外にも、翻訳技術の向上により、海外からの標的型攻撃メールを中心としたサイバー攻撃を容易に行うことが出来るようになった。

日々進化するサイバー攻撃の脅威などに対し、被害に遭わないようにするために、情報セキュリティ対策は、日頃から最新情報の収集を心がけて行う必要がある。

③政府の情報セキュリティ対策の現状

情報セキュリティの脅威が深刻化している状況を受け、２０１４年１１月に、サイバーセキュリティ基本法が成立し、２０１５年1月内閣には「サイバーセキュリティ戦略本部」が、内閣官房に「内閣サイバーセキュリティセンター（NISC)」が設置された。また、２０１５年１２月に経済産業省では、独立行政法人情報処理推進機構（以下、ＩＰＡ）と共に、情報セキュリティ対策に対する経営者への啓発のための「サイバーセキュリティ経営ガイドライン」の策定が行われ、総務省では実践的なサイバー防御演習（ＣＹＤＥＲ）が実施されるなど様々な取組みがなされている。

④中小・小規模事業者の情報セキュリティ対策の課題

サイバー攻撃の対象となるのは公的機関や大企業だけではない。ネットバンキングの不正送金事件の増加や、クレジットカードの情報の不正取得などで実際に中小・小規模事業者も被害を受けている例もある※注－２。また、大企業に対するサイバー攻撃を行う際には、中小・小規模事業者などの取引先を踏み台にして、ターゲット企業のシステムに入り込むケースもある。

２０１５年2月にＩＰＡが行った調査によると、中小・小規模事業者は大企業と比較し、情報セキュリティ対策に関する取組みを行っている割合が低いとの結果が出ている。中小・小規模事業者は、日本国内企業全体の９９．７％を占めており日本経済の屋台骨を支えていることから、今後中小・小規模事業者の情報セキュリティ対策を抜きに日本経済の持続的な成長は考えられない。日本経済の持続的な発展を図るうえで、速やかに改善しなければならない。

⑤法改正等に伴う中小・小規模事業者への影響

一方、２０１５年９月には個人情報保護法の改正、２０１６年１月よりマイナンバー制度が開始されるなど、中小・小規模事業者を含めた全ての企業に情報セキュリティ対策が求められるようになった。

※注－２：都内のカー用品小売店（資本金１，０００万円）ではサイバー攻撃により２８，２１２件のクレジットカード情報が流出した事例がある。

事業者が安定した経済活動を継続するために、社会環境の重大な変化を認識しつつ、適切な情報セキュリティ対策を行うことは極めて重要である。

しかし、中小・小規模事業者は「ヒト・モノ・カネ」の経営資源が十分とは言えず、現状では情報セキュリティ対策を満足に行うことは困難である。

⑥中小・小規模事業者が保有する知的財産の保護への課題

２０１５年７月に不正競争防止法の一部が改正された。背景には、我が国の企業の営業秘密が国内外に流出する事案が顕在化したことがあるが、新興国に我が国の営業秘密が流出するリスクは、国際競争力低下にもつながることが懸念されることから、技術情報や顧客名簿などの営業秘密の漏えいに、歯止めをかけることが必要である。

その一方、加害者となるリスクもある。例えば、中途採用者より前社の営業秘密が持ち込まれ、それを使用した場合、営業秘密侵害の訴訟を受ける可能性がある。万が一、米国企業の営業秘密を侵害したと問われた場合、巨額の賠償金を請求される恐れすらある。

これらのリスクは中小・小規模事業者も例外ではない。中小企業の特許出願件数は２０１１年より毎年増加傾向にあることからも、（※図１）　保有する技術情報などの情報セキュリティ対策は喫緊の課題である。

図１

⑦東京オリンピック・パラリンピック等の国際的イベントに対する課題

２０１６年の伊勢志摩サミットを皮切りに、２０１９年にはラグビーワールドカップ、２０２０年東京オリンピック・パラリンピックの開催を控えている。これらは、日本のサービス・インフラを世界に示す絶好のチャンスであると同時に、何らかのセキュリティ上の事故が発生すれば、国の威信に関わる重大な事態となる。よって、情報セキュリティ対策は、大会を成功に導くためにも万全を期す必要がある。

以上の基本的な考えに基づき、より一層の中小・小規模事業者の情報セキュリティ対策を推進すべく、以下に記載する項目につき、格段の配慮が図られるよう要望する。

なお、東京商工会議所は、２０１６年1月１４日に警視庁、東京都商工会議所連合会、東京都商工会連合会、東京都中小企業団体中央会、公益財団法人東京都中小企業振興公社とサイバーセキュリティに関する相互協力協定を締結した。当所としても、中小・小規模事業者のサイバーセキュリティ意識の啓発活動などを初め、関係諸機関との連携を密にし、地域の総合経済団体として、中小・小規模事業者支援に尽力する所存である。

Ⅱ．意見項目

１．情報セキュリティ対策の意識向上・強化

①経営者の情報セキュリティ対策に関する意識の向上・強化

日本企業の情報セキュリティに対する意識は、国際的に比較して低い状況にある。プライスウォーターハウスクーパース株式会社が行った「グローバル情報セキュリティ調査®２０１５（日本版）」によると企業の情報セキュリティ投資額は、世界全体平均の年間４．２億円に対して、日本企業の平均は年間２．１億円と２倍の差がある。更に、ＩＰＡの調査によると中小・小規模事業者においては情報セキュリティに対する予算や体制の充実を検討する割合が大企業と比較すると低い傾向にある。※参考－１

情報セキュリティに対する予算や体制の意思決定を行うのは経営者であり、社内の情報セキュリティ対策を推進するには、経営者が積極的に取組む意識が、必要不可欠である。しかしながら、現状においては、情報セキュリティ対策は利益を生まない費用負担との認識であり、情報セキュリティに対する対策は後回しにされてきた。特に、人的・資金的に限りのある中小・小規模事業者はなおさらである。しかし、インシデント（問題）が発生した際は多大な労力と費用が発生するのみならず、取引先の情報などが流失した場合には信用の失墜にもつながり企業の存続に支障をきたすことから、情報セキュリティ対策を、重要な経営戦略の一環として捉え、経営者に情報セキュリティマインドを浸透させることが最も重要である。経営者は取引先に迷惑をかけてはいけないという共通認識がある。啓発を行う際には、顧客情報が流出することで、取引先に多大な被害がかかることを例示すれば理解が得やすくなると考える。

経営者のマインドが変われば、企業が一丸となって情報セキュリティ対策に取組むことが期待される。先ずは、経営者の情報セキュリティ対策に対する意識向上の啓発が望まれる。

※参考－１
ＩＰＡの調査では、情報セキュリティ対策について、今後、予算や体制を充実させる予定があるかという問いに対し、大企業は２７％があると回答したが、中小・小規模事業者は９．５％と大きな乖離が生じた。

②ＢＣＰ（Business Continuity Plan）への取込み

サイバー攻撃の手法は日々進化しており、１００％サイバー攻撃を防ぐことは非現実的であるが、実際に情報セキュリティにかかるインシデントが発生したことを想定して対策計画を立てることは、被害を最小限に食い止める上でも重要である。

中小・小規模事業者がＢＣＰを策定する際に、サイバー攻撃や情報漏えいなど情報にかかるインシデントについても緊急事態として取込むことが大切である。事態の重さを認識してもらうためにも、インシデント事例を紹介し、実際にどのくらいの損害が発生するか示すことで被害の大きさのイメージを容易にさせることが必要である。

③中小・小規模事業者も活用できる「サイバーセキュリティ経営ガイドライン」の解説などの策定

２０１５年１２月に経済産業省では、ＩＰＡと共に、「サイバーセキュリティ経営ガイドライン」を策定したが、ガイドラインの対象から小規模事業者が除かれている。しかし、マイナンバーの施行や、個人情報保護法の改正により中小・小規模事業者にとっても情報セキュリティ対策を講じることは必須となった。よって、中小・小規模事業者も活用できる解説などを策定することが望まれる。

策定される際には、中小・小規模事業者の目線を意識し、簡潔かつ理解しやすい内容にされること。また、業種・業態に応じたインシデントやその対応例を示すなど、事業規模のレベル感を踏まえ、きめ細やかな内容にとするよう留意されたい。

④情報セキュリティ対策に対する啓発

情報セキュリティ対策は、大掛かりな設備導入やシステム導入を行わなくても、出来ることはある。具体的には

・ＵＳＢなどの情報機器の持込・持出を制限する
・仕事の持ち帰りを含めてデータの持ち出しを制限する
・機密情報にはマル秘表示を行い、秘密情報の認識を分かりやすくする
・防犯カメラの設置やレイアウトの工夫する
・端末を使用する際のパスワードの設定を行う

・担当者別（システム管理者・役職者など）のアクセス制限の設定を行う
・個人情報が含まれたファイルにはパスワードを設定する
・パソコンとデスクにはワイヤーロックをかける
・ＳＮＳ（social networking service）の利用方法について教育する
・ＯＳ（Operating System）やアプリケーションなどの最新のアップデート更新
・最新の攻撃手法やウィルスをチェックする
・ＪＶＮバージョンチェッカなどを利用して自社のパソコンの脆弱性をチェックする
・社内データのバックアップを取っておく　等

容易且つ即効性の高い情報セキュリティ対策はある。

しかし、このような簡易な情報セキュリティ対策でも、中小・小規模事業者は取組んでおらず※参考－２　中小・小規模事業者の従業員の目線に合わせた、必要最低限行うべき情報セキュリティ対策の啓発が望まれる。また、情報漏えいの原因は外部からの攻撃のみならず「人」に起因することが多いため、人の心理特性（業務の忙しさ、煩雑さに起因するインシデント）にも着目されたい。さらに、スムーズな情報セキュリティ対策の導入につなげるためにもパッケージ化した対策方法をいくつか例示することは効果的であろう。

※参考－２
ＩＰＡの調査では、情報セキュリティに関する取組みについての問いに対し、機器や記録媒体の持込・持出の制限を行っている中小企業は３１．６％という結果が出た。

⑤中小・小規模事業者支援機関の取組み支援

東京商工会議所では、２０１０年度から２０１５年度にかけて無料にて情報セキュリティ対策セミナーを計２７回実施し、累計３，１３１名が参加した。更に多くの企業経営層にセキュリティマインドの向上を効率的に図りつつ、日々進化するサイバー攻撃に対抗するためにも中小・小規模事業者支援機関による継続した情報セキュリティ対策セミナーの実施は必要であることから、中小・小規模事業者支援機関によるセキュリティ対策セミナーの実施に際し、支援の拡充が望まれる。

２．情報共有・連携の強化

〇被害後の情報共有及び官民の情報連携の強化

サイバー攻撃の手法は日々進化しており、情報セキュリティ対策も常に更新していかなければいけない。そのため、政府機関と企業・業界団体などが連携して、ウィルスの種類・脆弱性などの攻撃の手法を分析し、対処方法を打ち出すこ

とが新たな被害を食い止めることにつながる。現在ＩＰＡより、ホームページを通じて各種情報提供が行われているが、今後も引続き最新の攻撃手法や被害状況などを広く情報提供され対処方法を公開されたい。事例収集にあたっては各コンピュータセキュリティ企業や一般社団法人 ＪＰＣＥＲＴ コーディネーションセンターなどの機関との情報共有の強化が有効と考える。併せて、一般から些細な事象でも、おかしい・怪しいと感じた際には通報を受付・収集できる環境を整備することも有効と考える。

また、情報共有の一環として、ＩＰＡやプロバイダー企業と協力して中小・小規模事業者向けにトレンドに合わせた訓練やワークショップを実施することも望まれる。

実際にサイバー攻撃を疑似体験し、実感することで強く情報セキュリティの重要性が認識されるであろう。

他方、各種メディアを通じて広くあまねく情報セキュリティに関する周知活動を行うことも重要である。

３．相談体制の周知ならびに拡充

①ＩＰＡ相談窓口の積極的なＰＲ及び相談体制の拡充

ＩＰＡでは「情報セキュリティ安心相談窓口」を設けており、電話やＦＡＸ、メールにて相談できる体制がある。マルウェアや不正アクセスの被害に遭った際に、相談窓口があることは、非常に有益であることから、まず「情報セキュリティ安心相談窓口」が認識されるよう、十分なＰＲが望まれる。

また、「情報セキュリティ安心相談窓口」の電話相談は平日の１０時から１２時及び１３時３０分から１７時となっているが、インシデントは時を選ばず発生することが想定される。したがって、例えば電話相談については時間延長や、利便性の向上及び認知拡大のため、覚えやすい電話番号の設定を検討されたい。

②対面型による相談窓口の設置及び拠点化

先述の通り、ＩＰＡでは「情報セキュリティ安心相談窓口」を設けており、電話やＦＡＸ、メールにて相談できる場はあるものの、対面での個別具体的な対応は難しい状況にある。情報セキュリティ対策の相談内容は企業によって千差万別であり、身近な場所で対面による相談ができる場があることは情報セキュリティ対策を講じる際に、または被害に遭った時にも非常に有効と考える。

相談体制の充実を図るため、専門家との対面による相談窓口拠点の設置及び専門家派遣などの制度の拡充が望まれる。また、その際に専門家として「情報処理安全確保支援士」（Ｐ１０ 意見項目４ ⑤参照）の活用が有効と考える。

なお、東京商工会議所では、窓口相談及び専門家派遣を実施しており、相談体制構築に今後も尽力していく。

４．情報セキュリティ人材の確保・育成

①中小・小規模事業者が情報システム担当者を雇用する際の支援

現在、情報セキュリティ人材は不足している状況にあり、※参考－３　また、企業の規模が小さくなるほど、情報セキュリティ対策の担当者・部門を置いている割合が少なくなるとの結果が出ている。情報セキュリティ人材が不足している状況の中で、資金に限りのある中小・小規模事業者が担当者を確保することは困難なことから、中小・小規模事業者がＩＴ担当者を新たに雇い入れる場合の奨励金制度などの拡充が望まれる。

※参考－３

２０１４年７月に発表されたＩＰＡの報告によると、情報セキュリティ人材は約２６．５万人いるが、そのうち約１６万人はスキル不足であり、また絶対数としてもあと８万人は必要とのことであり、結果的に２４万人に教育が必要。

②人材の供給支援

情報セキュリティ人材が不足している中、情報セキュリティ人材を効率的に行き渡らせるにはワンストップで効率的に人材を供給できる仕組みが有効である。既にある人材バンクなどを活用し、情報セキュリティ人材を供給できる体制を官民が連携して推進する必要がある。

③人材育成の環境整備

安定した情報セキュリティ対策のできる人材を維持・確保するためには早期からのＩＣＴ教育が必要である。これは、人材の「量的拡大」と「質的向上」を図る上でも重要である。スマートフォンの普及により最近は小・中学生でもＳＮＳやブログによる情報の受発信が容易な環境にある。※参考－４

また、世界にも通用する専門技術を持った人材の養成が必要であり、特にサイバー空間に国境はないので、グローバルに対応できる専門技術者が求められていることから、産官学の連携も含めて次の取組みを推進されたい。

- 小・中学校からの早期のＩＣＴ教育の実施
- グローバル水準のＩＣＴ専門能力を育成するための高等教育機関の設置

※参考－４

総務省　平成２７年版情報通信白書によると１０代のスマートフォンの利用率は７８．５％であり、パソコンの同年代の利用率は７６．３％である。

また、２０１５年の文部科学省の調査では、小学生のスマートフォン所有率の全国平均は５８．０％、最も所有率の高い東京都では６８．１％となっている。

④新設される「情報セキュリティマネジメント試験」の普及・啓発

経済産業省では、２０１６年４月より情報セキュリティマネジメント試験が導入されることから、日本国内におけるセキュリティマインドの底上げが期待される。また、同資格は、「ＩＣＴによる対策（技術面の対策)」だけではなく、適切な情報管理など「人による対策（管理面の対策)」について、業種を問わず幅広い対応ができることから、国内の情報セキュリティ対策の推進を図るうえで非常に有益な資格と考える。これらの試験を普及し、情報システムを扱う者においてはスタンダードライセンスとすべく、十分なＰＲが望まれる。普及に際して、例えば情報システム担当者として最低限求められるスキルの指標としての確立や、ＢＣＰ策定の際の取引条件の項目の一つの要件として推奨することなどが考えられる。

⑤新設される「情報処理安全確保支援士」の普及及び活用促進

経済産業省では２０１７年度より情報処理安全確保支援士制度の創設が検討されている。最新のセキュリティに関する知識・技能を備えた、高度かつ実践的な人材を創出されることが期待される。同資格保有者を増やし、活用することで高度な情報セキュリティ人材の増加及び確保につながることから、情報処理安全確保支援士資格の積極的な普及及び活用を促進されたい。将来的には、一定の従業員数を超える企業に対しては、情報処理安全確保支援士の設置の義務付けを検討されたい。

また、情報処理安全確保支援士は、社内情報セキュリティ担当者のみならず社外でも有効な相談が可能な「かかりつけの相談者」のような人材として活躍・活用されることが望まれる。

５．情報セキュリティ対策に必要な設備導入の促進

〇中小・小規模事業者が情報セキュリティ対策ソフト及び設備機器を導入する際の支援

中小・小規模事業者が情報セキュリティ対策を行うにあたって物理的な面では、新たなソフトの購入やシステム導入・更新、ファイヤーウォール、防犯カメラなどの設備の設置を要するケースが想定される。しかし、これらに掛かる費用は売上に直結するものではなく、利益を生まない負担であり、必要性が理解できても導入をためらってしまうことが考えられる。情報セキュリティ対策に必要な設備導入を促進すべく、次の支援を推進されたい。

- 情報対策設備導入時の一部購入費の助成
- 小規模事業者持続化補助金における、補助対象事業を情報セキュリティ対策費用も含めた拡充

➢情報セキュリティ対策設備購入時の低利による制度融資の設計
➢情報セキュリティ対策設備に対する中小企業投資促進税制の期限（２０１７年３月３１日まで）延長及び上乗せ措置の拡充

６．被害拡大防止の支援

○被害後に行うデジタルフォレンジック（データの保全・復元・解析）に対する支援

サイバー攻撃などの被害にあった際に、原因究明及び被害状況の確認を行うことは被害拡大を防止する上でも非常に重要な作業である。パソコンなどの情報端末によるインシデントが発生した際、コンピュータウィルスやデジタルデータは目に見えるものではないため、デジタルフォレンジック（データの保全・復元・解析）を行うことが有効である。しかし、デジタルフォレンジックは高度な技術を要するので外部に委託することになるが、その際は高額な費用が発生する。資金面で限りのある中小・小規模事業者は、被害を放置したままになりかねない。被害拡大の防止を図るべく、デジタルフォレンジックにかかる費用の支援を検討されたい。

７．国際イベント・法改正等に対する取組み

①２０２０年東京オリンピック・パラリンピックへの対応

２０２０年に、東京オリンピック・パラリンピックが開催される。オリンピック・パラリンピックは国民的行事であり、中小・小規模事業者においても大きなビジネスチャンスである。しかし、同時にボット（コンピュータを外部から遠隔操作するためのバックドア型不正プログラム）などを利用した、サイバー攻撃の対象とも成り得る。東京オリンピック・パラリンピックの成功に導くべく、サイバー空間の監視機能の強化及びインシデント発生時に早急に対処できるような体制の構築が望まれる。

②マイナンバー制度、改正個人情報保護法（５０００件要件撤廃）への対応

２０１５年９月に個人情報保護法の改正により個人情報数５０００件以下の事業所の適用除外が廃止された。また、２０１６年１月よりマイナンバー制度が開始され、中小・小規模事業者のほとんどが新たに同法への対応が必要となった。これにより、個人情報保護の対策に伴う業務負担が増加することになる。

マイナンバー制度については、既に内閣府より中小企業向けポイント資料（入門編）やマイナンバー導入チェックリストを公表されている。また、経済産業省からも「中小企業における マイナンバー法の実務対応」が公表されていることから、これらの更なる周知・ＰＲが望まれる。

また、個人情報保護法の改正についても同様の中小・小規模事業者にも理解し

やすい資料を作成・公表されたい。

③中小・小規模事業者が保有する知的財産保護への対応

東京商工会議所において、中小・小規模事業者を対象に知的財産に関する調査を行ったところ、殆どの企業が営業秘密の管理をしていない、若しくは管理しているが自信がないという結果であり※参考－５　営業秘密が盗まれたり、流失したことがある企業は１７．２％存在する。

経営資源が限られている中小・小規模事業者にとって知的財産は自社の競争力を高め、他社との差別化を図ることができる大切な宝である。しかし、知的財産が管理できておらず、そして流出されるような状況は早急に改善しなければならない。

まずは中小・小規模事業者の知的財産に対する情報セキュリティも含めた意識向上が必要と考える。経済産業省では２０１６年２月に「秘密情報の保護ハンドブック～企業価値向上に向けて～」を策定されたが、中小・小規模事業者向けの普及啓発資料を充実されることを望む。その際には、中小・小規模事業者が手に取りやすいこと、及び専門的な用語を極力使わず、誰にでも理解しやすい内容にされることを留意されたい。

※参考－５

２０１５年７月の東京商工会議所会員の製造業の中小・小規模事業を対象に知的財産に関する調査をしたが、８１．１％の企業が営業秘密（特許にしていない秘密の技術、ノウハウ、顧客名簿等）を管理していない・わからない、管理しているか自信はないとの結果であった。

以　上

２０１６年度第３号
２０１６年４月１４日
第６８２回常議員会決議

東京中小企業サイバーセキュリティ支援ネットワーク（イメージ）

Tcyss = Tokyo Cyber Security Support network
for small and medium enterprises