中小企業の情報セキュリティ対策強化に向けて

江　島　将　和
（独立行政法人情報処理推進機構
セキュリティセンター企画部
中小企業支援グループ）

1. はじめに

IoTやAIといった技術により実現される「Society5.0」、「Connected Industries」では、データを介したつながりから新たな付加価値が生み出されていくことが期待されている。一方で、企業間・産業間がつながることによって、ネットワーク化されたサプライチェーン上に攻撃の起点が広く拡散していくことになり、悪意のある者にとって新たな攻撃の機会となる恐れがある。

サイバー攻撃に対して危機意識が十分でない中小企業も少なくないが、大企業だけでなく、サプライチェーンに参加する地域の中小企業であっても、例外なくサイバー攻撃の脅威にさらされている実情が徐々に明らかになっている。このため、サプライチェーンを構成する中小企業の情報セキュリティ対策の強化は、我が国の産業に対する世界の信頼に直結する重要な課題である。

本稿では、中小企業の情報セキュリティ対策強化に向けて独立行政法人情報処理推進機構（以下、IPA）が取り組む情報セキュリティ対策支援事業について解説する。

2. 中小企業における情報セキュリティの実態

IPAでは、2016年度に「中小企業における情報セキュリティ対策に関する実態調査」（以下、実態調査）を実施し、情報セキュリティ対策の実施状況やインシデント発生状況、情報セキュリティ対策強化に向けての課題等を調査した。

情報セキュリティに関する脅威について、コンピュータウイルスを脅威と認識している企業は89.1%、不正アクセスを脅威と認識している企業は85.6%と高い割合を示した。一方で、技術的対策の実施状況について、ウイルス対策ソフトの導入は80.4%、ファイアウォールの導入は33.7%、ワンタイムパスワード等の個人認証の強化は15.7%と対策は十分に進んでいない。また、人的・組織的対策の実施状況についても、情報セキュリティ対策の担当者（兼務を含む）がいる企業は38.4%、セキュリティポリシー（セキュリティの規定やルール）を文章化している企業は14.0%と対策は十分に進んでいない。これらを企業規模別で見ると、規模が小さい企業ほど対策が進んでおらず、企業規模による差が著しい状況が明らかとなった。自社の情報セキュリティ対策が十分と認識する企業は39.3%であり、情報セキュリティ対策をさらに向上させるためには、「従業員の情報セキュリティ意識向上」や「経営者への情報セキュリティ意識向上」が重要であると考えている。

情報セキュリティ被害（ウイルス感染）について、「ウイルスをまったく発見しなかった・感染していない」が最も多く51.9%、次いで「ウイルスを発見したが、感染には至らなかった」が26.7%、「ウイルスに感染した」が5.1%であった。これを企業規模別で見ると、規模が大きい企業ほどウイルス感染若しくは発見している割合は高く、サイバー攻撃（ウイルス感染を除く）や内部不正に関する情報セキュリティ被害についても同様の傾向を示している。一見、規模が

大きい企業ほど情報セキュリティの脅威が大きいことを示しているように見えるが、情報セキュリティ対策が進んでいない小規模企業がサイバー攻撃や被害に気付けていない可能性も考えられる。

そこで、2019年度及び2020年度の「中小企業向けサイバーセキュリティ対策支援体制構築事業（サイバーセキュリティお助け隊）」において、中小企業におけるサイバー攻撃の実態把握を行った。本事業では、中小企業に対してUTM（Unified Threat Management）やEDR（Endpoint Detection and Response）等のセキュリティ機器を設置することで、外部からの不審なアクセスや不正プログラムによる内部から外部への不正通信等のサイバー攻撃を検知及び防御し、必要に応じて駆付け支援を行った。

2019年度は全国8地域で中小企業1,064社を対象に検証を行った結果、中小企業においても業種や規模を問わず例外なくサイバー攻撃を受けている状況が確認されるとともに、検知及び防御のための対策や社内体制の構築ができていない企業が多いことが確認された。また、2020年度は15の地域・産業分野で中小企業1,117社を対象に検証を行った結果、2019年度と同様に、業種や規模を問わずサイバー攻撃の脅威にさらされており、ウイルス対策ソフト等の既存対策だけでは防ぎきれていない実態が明らかとなっている。

3. 中小企業に向けた情報セキュリティ支援策

IPAでは前項の調査や専門家による研究会等を踏まえ、中小企業の情報セキュリティ対策強化に資する制度や資料等を作成し、公開及び運用することで、中小企業に向けた情報セキュリティ支援策を提供している。本項では主な支援策を解説する。

⑴ 中小企業の情報セキュリティ対策ガイドライン

中小企業の情報セキュリティ対策ガイドラインは、中小企業の経営者及び対策実践者を対象に、情報セキュリティ対策に取り組む際に経営者が認識し実施すべき指針と、社内において対策を実践する際の手順や手法をまとめたものである。本編2部と付録により構成されている。

第1部「経営者編」では、情報セキュリティ対策を進めていくうえで経営者が認識すべき「3原則」と実行すべき「重要7項目の取組」について説明している。第2部「実践編」では、情報セキュリティ対策の進め方についてステップアップ方式で具体的に説明している。付録として、実践編を進めていくうえで必要となる情報資産管理台帳のひな形や情報セキュリティ関連規程のサンプルを提供しており、付録を活用することで専門人材が不足する中小企業でも対策を進めていくことができるようになっている。

⑵ セキュリティ対策自己宣言制度「SECURITY ACTION」

SECUIRITY ACTION（セキュリティアクション）は、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である。「中小企業の情報セキュリティ対策ガイドライン」の実践をベースに2段階の取組目標が設定されており、取組目標に応じたロゴマークを無料で使用することができる。

1段階目「一つ星」では、脆弱性対策、ウイルス対策、認証強化、共有設定の見直し、脅威情報収集という基本的だが効果的な5つの対策「情報セキュリティ5か条」を取組目標としている。2段階目「二つ星」では、25個の診断項目に答えるだけで自社の情報セキュリティの問題点を簡単に把握できる診断ツール「5分でできる！情報セキュリティ自社診断」を使って自社の対策状況を把握したうえで、「情報セキュリティ基本方針」を定めて外部に公開することを取組目標としている。

SECURITY ACTIONを宣言することで、情報セキュリティ対策の取り組みの「見える化」を図ることができ、社内の意識付けや社外への信頼性のアピール等に活用することができる。また、経済産業省が実施するIT導入補助金や地方公共団体等が実施する補助金制度の申請要件、損害保険会社のサイバー保険の割引条件等としても活用されており、今後も更なる活用が期待されている。2021年9月時点の宣言数は17万件を超えている。

⑶　セキュリティプレゼンター制度

セキュリティプレゼンター制度とは、IPAのセキュリティ対策資料等を活用して、中小企業等に対して情報セキュリティの普及啓発を行う人材を「セキュリティプレゼンター」として登録する制度である。

IPAではセキュリティプレゼンターに対してカンファレンスやポータルサイトによる情報提供、勉強会による指導力向上を図ることで、セキュリティプレゼンターを通じた地域の中小企業支援を推進している。セキュリティプレゼンターには、情報処理安全確保支援士やITコーディネータ、中小企業診断士等の資格を有する専門家の登録が多く、2021年11月時点の登録数は1,600名を超えている。情報セキュリティ人材が不足する中小企業において、地域の身近な専門家としてセキュリティプレゼンターの活用が期待される。

⑷　情報セキュリティ対策支援サイト

情報セキュリティ対策支援サイトは、情報セキュリティ対策を「知りたい」「学びたい」「始めたい」「続けたい」中小企業と、それを後押しするセキュリティプレゼンターの活動をサポートするポータルサイトである。

「5分でできる！情報セキュリティ自社診断」や「情報セキュリティ対策ベンチマーク」の設問に答えることで自社の対策状況を把握することができ、診断結果に即した推奨資料やツールを入手することができる。また、従業員が情報セキュリティ対策について学習できるe-Learning「5分でできる！情報セキュリティポイント学習」や地域で活動するセキュリティプレゼンターの検索機能等を無料で利用することができる。

⑸　サイバーセキュリティお助け隊サービス審査登録制度

サイバーセキュリティお助け隊サービス審査登録制度は、中小企業のサイバーセキュリティ対策に不可欠な各種サービス（相談窓口、異常の監視、緊急時の対応支援、簡易サイバー保険等）をワンパッケージで安価に提供する民間サービスを「サイバーセキュリティお助け隊サービス」として審査・登録する制度である。

サービス基準を充足するサービスに「サイバーセキュリティお助け隊マーク」を付与することで普及を促進し、幅広い中小企業において無理なくサイバーセキュリティ対策を導入・運用することを支援している。

4. 中小企業に向けた情報セキュリティの普及啓発活動

IPAでは、前項の支援策について、IPA単独の普及啓発に加えて、公的機関や商工団体等の他組織との連携を図り普及啓発に取り組んでいる。本項では主な普及啓発の枠組みを解説する。

⑴　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

2017年2月、IPA及び中小企業と関わりの深い商工団体・士業団体の全国組織、IT関連団体及び関連する施策の実施機関である独立行政法人は、経済産業省・中小企業庁の協力の下、強固な連携により、各団体･組織の機能や特徴を活かしながら、中小企業の自発的な情報セキュリティ対策への取り組みを促す活動を推進することを目的とした「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」を発出した。

本宣言による活動において“自発的な情報セキュリティ対策を促す”ための核となる取り組みとして、中小企業自ら取り組みを宣言する制度「SECURITY ACTION」を創設し、宣言企業の拡大を通じた情報セキュリティの普及啓発活動を展開している。

⑵　サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）

2020年11月、主要経済団体のリーダーシップの下、多様な産業分野の団体等が集まり、サプライチェーン全体でのサイバーセキュリティ対策の推進を行うことを目的とした「サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）」が設立された。本コンソーシアムでは、サイバーセキュリティ体制の構築が十分でない中小企業の動機付けも含む、サプライチェーン全体でのサイバーセキュリティ対策の強化に向けた取り組みの検討や推進が行われており、2021年10月末時点で175会員（経済団体、業種別業界団体等）が参加している。IPAは、本コンソーシアムの事務局を担い、産業界の取り組みを支援するとととともに、産業界との対話を強化して、サイバーセキュリティ対策の推進運動へとつなげている。

5. おわりに

本稿では、中小企業における情報セキュリティの実態とIPAが提供する情報セキュリティ支援策、普及啓発活動を基にIPAが取り組む情報セキュリティ対策支援事業を解説した。

中小企業は情報セキュリティ対策に十分な経営資源を割り当てることができないという不利を抱える一方で、経営者から従業員の顔が見えるため、経営者が担当者や従業員に対策を指示し、その結果について直接報告を受けることができ、企業が一丸となって対策を推進するうえで有利な条件を備えている。IPAが取り組む情報セキュリティ対策支援事業を活用することで、サプライチェーンを構成する中小企業の情報セキュリティ対策強化の実現を願いたい。

【参考文献】

○2016年度中小企業における情報セキュリティ対策に関する実態調査 調査報告書
https://www.ipa.go.jp/security/fy28/reports/sme/index.html
○令和元年度中小企業向けサイバーセキュリティ事後対応支援実証事業 成果報告書
https://www.ipa.go.jp/security/fy2019/reports/sme/otasuketai_houkoku.html
○令和2年度中小企業向けサイバーセキュリティ対策支援体制構築事業 成果報告書
https://www.ipa.go.jp/security/fy2020/reports/sme/otasuketai_houkoku.html
○IPA中小企業向け制度・コンテンツなどのご案内
https://www.ipa.go.jp/security/keihatsu/sme/index.html