知って対策
リスクに備える

special 2

中小企業の情報セキュリティ対策

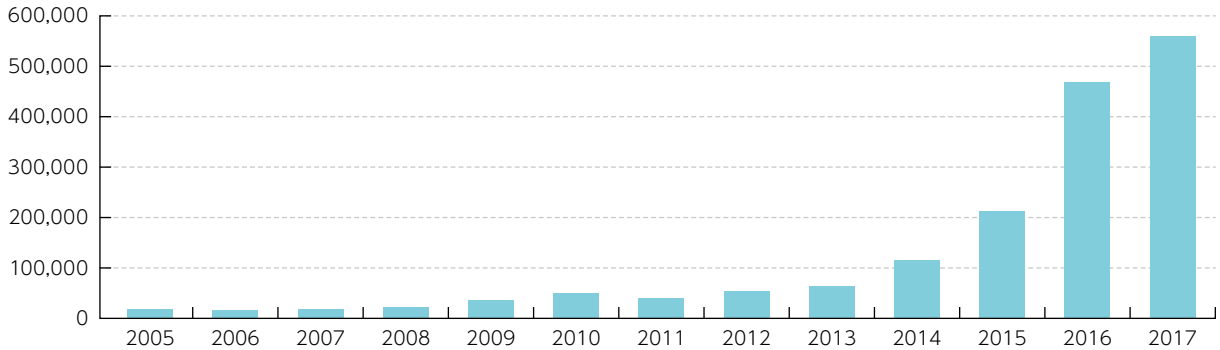
企業等の組織を狙ったサイバー攻撃は増加しており、その手口はますます巧妙化しています。しかし、それを防御するための備えが十分にできていない企業等も多く、特に中小企業における対策は進んでいないのが現状です。

本稿では、中小企業が行うべき情報セキュリティ対策について解説します。

Ⅰ 最近のサイバー攻撃の傾向

図表1は、国立研究開発法人情報通信研究機構（ＮＩＣＴ）が構築した大規模サイバー攻撃観測網（ダークネット観測網）にて観測された、サイバー攻撃関連通信に関するグラフです。１ＩＰアドレス当たりの年間総観測パケット数を表したもので、サイバー攻撃関連の通信がこの数年増加していることがわかります。図表2は、最近発生したサイバー攻撃の事例です。最近のサイバー攻撃の傾向として、特定の組織をターゲットにして、金銭や機密情報等の搾取を目的とする攻撃が

[図表1] 1IPアドレス当たりの年間総観測パケット数



出典：国立研究開発法人情報通信研究機構「NICTER観測レポート2017の公開」

増えていることが挙げられます。独立行政法人情報処理推進機構（ＩＰＡ）が２０１８年４月に発表した「情報セキュリティ10大脅威２０１８」では、組織の脅威の上位3つが「1位：標的型攻撃（※1）による被害」「2位：ランサムウェア（※2）による被害」「3位：ビジネスメール詐欺（※3）による被害」でした。サイバー攻撃では、ターゲットの組織の防御対策が強固だった場合、対策が弱い別の組織に最初に攻撃を仕掛け、そこを踏み台にして攻撃が行われることがあります。中小企業はこの踏み台として狙われる危険性が高く、知らぬ間に加害者側に加担することがあります。

Ⅱ 中小企業における情報セキュリティリスクと経営者の役割

サイバー攻撃の被害が発生した場合、経営者や担当者らが、個人情報保護法違反等の刑事罰や、高額な民法上の損害賠償責任を問われる可能性があります。さらには事業の中断や、社会や取引先からの信用失墜等のダメージを受けることも想定され、最悪の場合、事業の存続自体が危うくなりかねません。情報セキュリティ対策は経営者の責任であることを強く認識し、トップが先頭に立って対策を進める必要があります（図表3参照）。

[図表2]最近発生したサイバー攻撃の事例

2018年7月 某鉄道会社	サイバー攻撃により**ランサムウェア**に感染、業務ファイルサーバーに保存されているファイルに異常が見つかり、翌日には同サーバーに保存されたファイルへのアクセスができない状態となった。なお、列車運行に係る輸送システムや、定期券購入等に係る営業システム、ホームページ等はサーバーが別系統で管理されており、運行等への影響はなかった。
2018年6月 某洋菓子店	某洋菓子店の通信販売サイトが**不正アクセス**を受け、利用者のアカウント情報が流出していることが、第三者機関からの連絡で発覚した。利用者のメールアドレスとパスワード3万7,149件が海外のウェブサイトに掲載されていた。
2017年12月 某航空会社	取引先を装って送られた**偽のビジネスメール**による2件の振り込め詐欺にあい、総額約3億8千万円の被害を受けた。偽のメールは、振込先口座の変更と航空機のリース代などを請求する内容だった。いずれもその手口が巧妙であったため、担当者は信じ込み、普段と違う海外の銀行口座に振り込んだ。

出典：各種報道等より弊社まとめ

[図表3]経営者が認識すべき「3原則」と
経営者がやらなければならない「重要7項目の取組」

3原則	原則1	情報セキュリティ対策は**経営者のリーダーシップ**で進める
	原則2	**委託先の情報セキュリティ対策**まで考慮する
	原則3	関係者との情報セキュリティに関する**コミュニケーション**はどんなときにも怠らない
重要7項目	取組1	情報セキュリティに関する、**組織全体の対応方針を定める**
	取組2	情報セキュリティ対策のための**資源（予算、人材など）を確保する**
	取組3	担当者に必要と考えられる対策を**検討させて実行を指示する**
	取組4	情報セキュリティ対策に関する**定期・随時の見直しを行う**
	取組5	業務委託や外部サービスを利用する場合は、情報セキュリティに関する**責任範囲を明確にする**
	取組6	情報セキュリティに関する**最新動向を収集する**
	取組7	緊急時の**社内外の連絡先や被害発生時の対処について準備しておく**

出典：独立行政法人情報処理推進機構
「中小企業の情報セキュリティ対策ガイドライン」より弊社作成

[図表4]情報セキュリティ5か条

5か条	対　策　例
❶ OSやソフトウェアは常に最新の状態にしよう!	■Windows Update(Windows OSの場合)／ソフトウェア・アップデート(macOSの場合)／OSバージョンアップ(Androidの場合) ■Adobe Flash Player／Adobe Reader／Java実行環境(JRE)など利用中のソフトウェアを最新版にする
❷ ウイルス対策ソフトを導入しよう!	■ウイルス定義ファイルが自動更新されるように設定する ■統合型のセキュリティ対策ソフト(ファイアウォールや脆弱性対策など統合的なセキュリティ機能を搭載したソフト)の導入を検討する
❸ パスワードを強化しよう!	■パスワードは英数字記号含めて10文字以上にする ■名前や誕生日、簡単な英単語などはパスワードに使わない ■同じパスワードをいろいろなウェブサービスで使い回さない
❹ 共有設定を見直そう!	■クラウドサービスの共有範囲を限定する ■ネットワーク接続の複合機やカメラ、ハードディスク(NAS)などの共有範囲を限定する
❺ 脅威や攻撃の手口を知ろう!	■IPAなどのセキュリティ専門機関のウェブサイトやメールマガジンで最新の脅威や攻撃の手口を知る ■利用中のインターネットバンキングやクラウドサービスなどが提供する注意喚起を確認する

出典：独立行政法人情報処理推進機構「中小企業の情報セキュリティ対策ガイドライン」より弊社作成

Ⅲ 中小企業が取り組むべき情報セキュリティ対策

中小企業の情報セキュリティ対策においては、まずは基本的な対策を徹底することが重要です。2017年に世界中で猛威を振るったランサムウェア「WannaCry」は、企業等において基本的な対策を行っていれば被害を防ぐことが可能だったと言われています。サイバー攻撃の手法は年々巧妙化・高度化しているものの、その対策には共通的な部分があり、IPAの「情報セキュリティ5か条」(図表4参照)はその基本的な対策をまとめています。情報セキュリティリスクの低減に非常に有効ですので、これらの対策から確実に行っていくことを強く推奨します。

(※1)標的型攻撃：メールの添付ファイルを開かせたり、悪意あるウェブサイトにアクセスさせて、PCをウイルスに感染させる。その後、組織内の別のPCやサーバーに感染を拡大され、最終的に業務上の重要情報や個人情報が窃取される。さらに、金銭目的な場合は、入手した情報を転売等されるおそれもある。

(※2)ランサムウェア：PCやスマートフォンに保存されているファイルの暗号化や画面ロック等を行い、金銭を支払えば復旧させると脅迫する犯罪行為の手口に使われるウイルス。さらに、ランサムウェアに感染した端末だけではなく、その端末からアクセスできる共有サーバーや外付けHDDに保存されているファイルも暗号化されるおそれがある。組織内のファイルが広範囲で暗号化された場合、事業継続にも大きな支障が生じる。

(※3)ビジネスメール詐欺(Business E-mail Compromise：BEC)：巧妙に細工したメールのやりとりにより、企業の担当者を騙し、攻撃者の用意した口座へ送金させる詐欺の手口。

■脚注1~3は、IPAのHPより引用。