中小企業いばらき

CONTENTS

November
December
11・12
2024 No.793

クローズアップ

●中小企業の情報セキュリティ対策

写真　「いばらきの旅とうまいもの展 in 東京」
（写真紹介、記事は表紙裏面ページに掲載）

発行　茨城県中小企業団体中央会
https://www.ibarakiken.or.jp/
〒310-0801　水戸市桜川2-2-35　電話029-224-8030（代）

表紙の紹介

「いばらきの旅とうまいもの展 in 東京」を開催

主催：中央会　後援：茨城県・一般社団法人 茨城県観光物産協会

中央会は12月４日から６日までの３日間、JR東京駅地下１階グランスタ東京内スクエアゼロで「いばらきの旅とうまいもの展 in 東京」を開催した。

同所での開催は本年で３回目の開催となり、県及び一般社団法人県観光物産協会の後援を受け、茨城アフターデスティネーションキャンペーン期間中に実施。県内の飲食料品、青果物及び観光地や宿泊施設を県外にPRするとともに、各事業者の販売促進を図ることを目的に、本会会員組合等が取り扱う日本酒、ほしいも、納豆、漬物、米菓、野菜などを販売するとともに、県内宿泊施設や観光名所、道の駅などのパンフレットを配布した。

出展した飲食料品の組合関係者からは「県外の販路開拓のきっかけとすることができた」などの声が聞かれた。

出品・出展組合（組合員等）

【日本酒】 吉久保酒造㈱、㈱月の井酒造店、須藤本家㈱、㈱笹目宗兵衛商店、磯蔵酒造㈲、明利酒類㈱、岡部㈾、㈱剛烈酒造、檜山酒造㈱、㈱家久長本店、㈱木内酒造1823（ビール・ウイスキー等も販売）、根本酒造㈱、㈾井坂酒造店、嶋崎酒造㈱、森島酒造㈱、菊乃香酒造㈱、㈾椎名酒造店、愛友酒造㈱、金門酒造㈱、㈱田中酒造店、㈲廣瀬商店、府中誉㈱、稲葉酒造、㈾浦里酒造店、来福酒造㈱、村井醸造㈱、㈱西岡本店、㈱武勇、㈱山中酒造店、野村醸造㈱、㈱竹村酒造店、青木酒造㈱、萩原酒造㈱、珂北酒造㈲

【ほしいも】 ㈱小池清嗣商店、㈲米屋、㈱マルヒ、㈲扇屋商店、㈱住谷商店、㈱照沼、永井農芸センター、㈱住谷公商店、㈱浜喜商店、㈱幸田商店、㈱ニチノウ飛田、大丸物産㈱

【食肉加工品】 ㈲筑波ハム

【米菓】 さ志まや製菓㈱

【漬物】 ㈱根本漬物、大平漬物食品、㈲額賀商事、㈱吉田屋

【佃煮】 あべ佃煮

【納豆】 ㈲菊水食品

【野菜】 ㈲茨城BM

【観光】 茨城県ホテル旅館生活衛生同業組合　等

（順不同）

中小企業の情報セキュリティ対策

近年、情報機技術が急速に進展し、企業経営においてもＩＴは欠かすことのできないツールとなっています。中小企業においても、電子商取引、電子決済やテレワークなどＩＴの活用が広がってきています。

一方で、サイバー攻撃手法の巧妙化などＩＴの活用による経営上のリスクも増大していますが、中小企業は大企業に比べ、情報セキュリティ対策が遅れている傾向にあります。

そこで、企業を維持発展していくためには、早急に情報セキュリティ対策を講じる必要があることから、本号では、情報セキュリティの脅威となる事象やその被害事例を紹介した上で、情報セキュリティ対策に係るツールや相談窓口等を紹介します。

Ⅰ．情報セキュリティ10大脅威2024（組織向け）

「情報セキュリティ10大脅威2024」は、令和５年に発生した社会的に影響が大きかったと考えられる情報セキュリティの脅威となる事象から、独立行政法人情報処理推進機構（IPA）が脅威候補を選出し、情報セキュリティ分野の研究者、企業の実務担当者などのメンバーからなる「10大脅威選考会」が情報セキュリティの脅威候補に対して審議・投票を行い、決定したもの。情報セキュリティ対策の普及を目的として平成18年から毎年公表している。

なお、順位が高いか低いかに関わらず、組織が置かれている立場や環境を考慮して優先度を付け、適切な対応を取る必要がある。

１位から10位の概要や事例などは次のとおり。

１位：ランサムウェアによる被害（９年連続９回目 ※平成28年以降の10大脅威での取扱）

「ランサムウェア」とは、「Ransom（身代金）」と「Software」を組み合わせた造語であり、ウイルスの一種である。

ランサムウェアに感染すると、データの暗号化や重要情報の窃取等の被害に遭い、さらにその調査や復旧に多額の費用と多くの時間が掛かる。また、業務やサービス提供の停止による損失や取引先からの信頼失墜の被害につながるおそれもあり、広く利用されているサービスがランサムウェアに感染すると、社会に大きな影響を与えることになる。

【被害事例】

「ランサムウェア感染によるサービス提供停止」

令和５年６月、システム開発およびクラウドサービス会社Ａが、データセンターのサーバーに不正アクセスされ、ランサムウェアに感染したことを公表した。この感染により、データが暗号化され、社会保険労務士向けクラウドサービスを提供できなくなった。約3,400人のユーザーに影響があり、オンプレミス（サーバーやソフトウェアなどの情報システムを使用者（ビジネス利用の場合は企業）が管理する設備内に設置し、運用する）で動作するパッケージ版を代替として提供した。また、インフラ設備の再構築費用やセキュリティ対策費用のコスト増、影響があったユーザーへの６月の請求を停止するといった対応により、業績予想を修正することとなった。

２位：サプライチェーンの弱点を悪用した攻撃（６年連続６回目）

組織には、サプライチェーンとの関係性が何らかの形で存在する。取引先や委託先、ソフトウェアやサービスの提供元、提供先と多岐に渡る。強固なセキュリティ対策が行われていて、直接攻撃が困難な標的組織に対し、そのサプライチェーンの脆弱な部分を攻撃者が攻撃する。

攻撃を受けた場合、機密情報の漏えいや信用の失墜等、様々な被害が発生する。また、自組織が攻撃を受け、足掛かりとされることで取引相手に損害を与えてしまい、取引相手を失ったり、損害賠償を求められたりするおそれがある。

【被害事例】

「業務委託先業者からの顧客情報漏えい」

令和５年１月、複数の保険会社が、業務委託先から顧客の個人情報が流出したことを公表した。原因は業務委託先の、適切なセキュリティ対策がされていないサーバーへの不正アクセスであった。流出した個人情報が海外のWebサイトに掲載されていたことで被害が発覚した。流出の規模は保険会社により異なるが、多いところでは約130万人分に及んでおり、調査や対処に追われた。

３位：内部不正による情報漏えい等の被害（９年連続９回目）

従業員や元従業員等の組織関係者による機密情報の持ち出しや社内情報の削除等の不正行為が発生している。また、組織内の情報管理の規則を守らずに情報を持ち出し、紛失や情報漏えいにつながるケースもある。組織関係者による不正行為は、組織の社会的信用の失墜や、損害賠償や業務停滞等による経済的損失を招く。また、不正に取得された情報を使用した組織や個人も責任を問われる場合がある。

【被害事例】

「元勤務先に不正アクセスし、社内情報を削除」

令和５年１月、電気計測機器等の製造会社Ｂの元従業員が電子計算機損壊等業務妨害罪等の疑いで警視庁に逮捕された。本従業員は退職後に元同僚や元上司のIDやパスワードを悪用し、社内ネットワークやクラウドに不正アクセスして、人事や技術、顧客に関する情報を削除していた。人間関係を理由に退職しており、嫌がらせが目的だったとみられている。データ復旧には約660万円を要した。

４位：標的型攻撃による機密情報の窃取（９年連続９回目）

標的型攻撃とは、特定の組織（企業、官公庁、民間団体等）を狙う攻撃のことであり、機密情報等を窃取することや業務妨害を目的としている。攻撃者は社会の変化や働き方の変化に合わせて攻撃手口を変える等、組織の状況に応じた巧みな攻撃手法で機密情報等を窃取しようとする。

窃取された機密情報が悪用された場合、企業の事業継続や国家の安全保障等に重大な影響を及ぼすおそれがある。また、データ削除やシステム破壊により企業等の活動が妨害されたり、その企業のサプライチェーンに属する関連組織への攻撃の踏み台にされたりすることもあり、組織の規模や業種に関わらず狙われるおそれがある。

【攻撃手口】

①メールへのファイル添付やリンクの記載

メールの添付ファイルやメール本文に記載されたリンク先にウイルスを仕込み、そのファイルを開封させたり、リンクにアクセスさせたりすることでPCをウイルスに感染させる。

②Webサイトの改ざん

攻撃者は標的組織が頻繁に利用するWebサイトを調査し、改ざんしておく。そして、従業員や職員がそのWebサイトにアクセスすることでPCがウイルスに感染する。

③不正アクセス

標的組織が利用するクラウドサービスやWebサーバー、VPN装置等の脆弱性を悪用し、不正アクセスを行い、そこから更に組織内部へ侵入する。

【被害事例】

「複数回のやり取りを伴う標的型メール攻撃」

令和５年10月、Ｃ大学は標的型攻撃メールにより教員が使用していたPCがウイルスに感染し、PC内の情報を窃取された形跡があることを公表した。令和４年７月に実在する組織の担当者を騙った人物から講演依頼のメールが届き、日程調整のため教員がやりとりをしている中でメールに記載されたURLをクリックしたところ、ウイルスに感染した。最終的に「講演が中止になった」との連絡があったため、教員は被害に気付かなかった。この攻撃により、教職員や学生等の個人情報や過去の試験問題等計4,341件が流出したおそれがある。

５位：修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）（３年連続３回目）

ソフトウェアの開発ベンダー等が脆ぜい弱性対策情報を公開する前に、脆弱性を悪用した攻撃が行われることがある。このような攻撃は、「ゼロデイ攻撃」と呼ばれている。ゼロデイ攻撃が行われた場合、ウイルス感染や情報漏えい等の直接の被害に留まらず、事業やサービスが停止するなど、多くのシステムやユーザーに被害が及ぶことがある。そのため、脆弱性対策情報が公開された場合は、早急な対応が求められる。

【攻撃手口】

〇ソフトウェアの脆弱性の悪用

開発ベンダー等が脆弱性対策情報を公開する前に、攻撃者は脆弱性を悪用して攻撃する。

【被害事例】

「ファイル圧縮ソフトに存在する脆弱性を利用したゼロデイ攻撃」

広く利用されているファイル圧縮ソフトＡに複数の脆弱性が存在しており、令和５年４月以降に一部の脆弱性がゼロデイ攻撃に悪用されていることがわかった。アーカイブファイル内の画像ファイルやテキストファイルのプレビューを行おうとすると、同名のフォルダ内に配置されたスクリプトを実行させることが可能になるという脆弱性であった。開発元は、脆弱性の修正をしたバージョンをリリースしている。

６位：不注意による情報漏えい等の被害（６年連続７回目）

システムの設定ミスによる非公開情報の公開や、個人情報を含んだ記憶媒体の紛失等、不注意による個人情報等の漏えいが度々発生し、組織はその対応に追われている。一度でも不注意により個人情報が漏えいしてしまうと、漏えいした組織の信用、信頼に大きな影響を与えるおそれがある。

【要因】

①情報を取り扱う人の情報リテラシーの低さ

自身が扱う情報の機密性や重要性等を理解していないため、不用意に外部へ情報漏えいしてしまう。

②情報を取り扱う際の本人の状況

体調不良や多忙等の状況により、情報を取り扱う従業員の注意力が散漫になり、メールの誤送信等のミスによる情報漏えい事故を起こしてしまう。

③組織規程および情報を取り扱うプロセスの不備

組織で規定している情報の取り扱いプロセスに不備があると情報漏えいが起きやすい。例えば、外部に情報を持ち出す際の確認手順や作業時の確認手順等に関するプロセスの不備が挙げられる。

④誤送信を想定した偽のメールアドレスの存在

組織が利用しているドメインと似たドメインのメールアドレス（ドッペルゲンガードメイン）を、第三者があらかじめ準備している。従業員がそのメールアドレスに誤送信したタイミングで情報が漏えいする。

【不注意による情報漏えいの例】

・メールの誤送信（宛先誤り、To/Cc/Bccの設定間違い、添付ファイル間違い等）
・Webサイトの設定不備（重要情報のマスキングの不備、公開ファイルや参照権限の誤り、クラウドの設定の誤り等）
・外部サイトへの安易な機密情報の入力
・重要情報を保存した情報端末（PCやスマートフォン等）・記録媒体（USBメモリー等）の紛失
・重要書類（紙媒体）の紛失

７位：脆弱性対策情報の公開に伴う悪用増加（４年連続７回目）

ソフトウェアやハードウェアの脆ぜい弱性対策情報の公開は、脆弱性の脅威や対策の情報を製品の利用者

に広く呼び掛けられるメリットがある。一方で、攻撃者はその情報を悪用し、脆弱性対策を講じていない当該製品を使用したシステムを狙って攻撃を行うおそれがある。近年では脆弱性関連情報が公開されるとすぐに攻撃コードが流通し、攻撃が本格化するまでの時間がますます短くなっている。

【攻撃手口】

①対策前の脆弱性（Nデイ脆弱性）を悪用

パッチや回避策が公開される前に発見されたソフトウェアの脆弱性を「ゼロデイ脆弱性」と呼び、パッチや回避策が公開され、そのパッチの適用や回避策を講じるまでの期間（N日）の脆弱性を「Nデイ脆弱性」と呼ぶ。特に、ソフトウェアの管理が不適切な企業は、未対応の時間（N日）が長くなるため、被害に遭うリスクが大きくなる。

②公開されている攻撃ツールを使用

公開された脆弱性に対する攻撃ツールは短期間で作成され、ダークウェブ上のWebサイト等での販売や、攻撃サービスとして提供されたりすることがある。

8位：ビジネスメール詐欺による金銭被害（7年連続7回目）

企業の従業員や経営者、または、取引先の関係者等になりすました攻撃者が、標的組織の従業員等へメールを送信する。それらのメールは本物のメールに酷似しているため、メールの受信者はなりすましメールを受信したと気付けないおそれがある。

その結果、メールの受信者は、あらかじめ攻撃者が用意した口座に送金をしてしまい、金銭的な被害が発生してしまう。

【攻撃手口】

①取引先との請求書の偽装

取引先等と請求に関わるやり取りをメール等で行っている際に、攻撃者が取引先になりすまし、攻撃者の用意した口座に差し替えた偽の請求書等をメールで送り付け、振り込ませる。

②経営者等へのなりすまし

組織の経営者等になりすまし、同組織の従業員に攻撃者が用意した口座へ金銭を振り込ませる。この時、攻撃者は事前に入手した経営者や関係している従業員の情報を利用し、通常の社内メールであるかのように偽装する。

③窃取メールアカウントの悪用

ウイルス感染や不正ログイン等により、従業員のメールアカウントを乗っ取り、取引実績がある組織の担当者へ偽の請求等を送り付け、攻撃者の用意した口座に金銭を振り込ませる。

メール本文は巧妙に偽装され、送信元が本物のアカウントであるため、受信したメールが攻撃であることに気付きにくい。

④社外の権威ある第三者へのなりすまし

弁護士等の社外の権威ある第三者になりすまし、組織の財務担当者等に対して攻撃者が用意した口座へ金銭を振り込ませる。

⑤詐欺の準備行為と思われる情報の窃取

ビジネスメール詐欺の準備行為として、標的組織の情報を窃取する場合がある。例えば、攻撃者が標的組織の経営者や経営幹部、または人事担当等の特定任務を担う従業員になりすまし、組織内の他の従業員の個人情報等を窃取する。

【被害事例】

「信頼できる取引先を騙るメール詐欺」

バイオベンチャー会社Dは、支払口座の変更依頼が書かれた、取引先の名を騙るメールに従い、虚偽の銀行口座に振り込みをしたことを公表した。その後も同様の振り込みをし、合計2回で総額2億円を振り込んだことも公表した。その取引先とは創業以来の付き合いがあり、信頼関係があったため、同社は振込先口座の変更依頼の理由を直接電話で確認していなかった。そのため、当面の再発防止策として、送金プロセスの見直しなどを挙げている。

9位：テレワーク等のニューノーマルな働き方を狙った攻撃（4年連続4回目）

令和2年以降、新型コロナウイルス感染症対策に伴い、テレワークが定着し、自宅のネットワークの利用や私有のPCやスマートフォンを利用することがある。それに伴い攻撃者はこのような業務環境を引き続き狙っており、業務環境に脆ぜい弱性があると、Web会議をのぞき見されたり、テレワーク用の端末にウイルスを感染させられたり、ウイルスに感染した端末から社内システムに不正アクセスされたりするおそれがある。

【攻撃手口】

①テレワーク用製品の脆弱性の悪用

VPN等のテレワーク用に導入している製品の脆弱性や設定ミス等を悪用し、社内システムに不正アクセスしたり、PC内の業務情報等を窃取したりする。また、Web会議サービスの脆弱な設定を悪用し、Web会議をのぞき見する。

②テレワーク移行時のまま運用している脆弱なテレワーク環境への攻撃

規則の整備やセキュリティ対策が不十分な状態で、急いでテレワークへ移行したまま運用されている脆弱なテレワーク環境を攻撃する。

【被害事例】

「在宅勤務のために用意したリモートアクセス経路より侵入の疑い」

腕時計製造会社Eはランサムウェアによる被害で顧客や取引先担当者等の個人情報が流出したことを公表した。同社ではコロナ禍において在宅勤務のために用意したリモートアクセス経路より侵入されたものと見ている。データセンターや国内拠点の一部サーバー内部に保存されていたデータを暗号化され、保有する約60,000件の個人情報が外部に流出した。

10位：犯罪のビジネス化（アンダーグラウンドサービス）（2年連続4回目）

サイバー攻撃を目的としたツールやサービスがアン

ダークグラウンドで取り引きされており、アカウントのIDやパスワード、クレジットカード情報、ウイルスなどが売買され、あまり攻撃スキルがなくてもハッキングなどの犯罪行為を行えるようになっている。また、話題のサービスのアカウント情報などが売買されており、ユーザーはアカウントの管理等の対策に一層努める必要がある。

【攻撃手口】

①ツールやサービスを購入した攻撃

アンダーグラウンドで購入したツールやサービスを利用して攻撃を行う。脆ぜい弱性の悪用やボットネットの利用等、ツールやサービスの種類によって攻撃方法は異なる。代表的なサービスとしてはランサムウェアを販売するサービスや、不正アクセスの手段を販売するサービスが確認されている。

②認証情報を購入した攻撃

アンダーグラウンドで購入したIDやパスワード等の認証情報を利用して、Webサービス等に不正ログインする。

【被害事例】

「国内製造業の情報がダークウェブに流出」

ＩＴセキュリティ会社Ｅは、国内の主要製造業30社について、ダークウェブへのアカウント情報漏えい状況調査結果を発表した。結果として今回調査した30社全てでダークウェブ上にアカウント情報や機密文書がアップロードされていることが判明した。特に製造業は、過去調査した金融機関、行政機関の結果と比較すると情報漏えい件数やハッキング数等においてすべて上回っていた。

参考：IPA「情報セキュリティ10大脅威 2024」解説書（https://www.ipa.go.jp/security/10threats/10threats2024.html）

各事象の対策などは、「情報セキュリティ10大脅威2024」解説書に掲載していますのでご覧ください。

Ⅱ．情報セキュリティ対策

1．「中小企業のセキュリティ対策ガイドライン第3.1版」

「中小企業の情報セキュリティ対策ガイドライン」は、個人事業主、小規模事業者を含む中小企業向けに情報セキュリティ対策に取り組む際の（1）経営者が認識し実施すべき指針、（2）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、経営者編と実践編から構成されている。

第3.1版は、新型コロナウイルス感染防止策によるテレワークの普及や、DX推進の両輪としての情報セキュリティ対策といった社会動向の変化などを踏まえ、具体的な対応策を盛り込むための改訂を行った。同ガイドラインはIPAのHP（https://www.ipa.go.jp/security/guide/sme/about.html）で公開している。

2．「中小企業のセキュリティ対策ガイドライン」等を活用した対策のステップ

STEP１　できるところから始める

「情報セキュリティ５か条」を参考に自社でできるところから始める。

STEP２　組織的な取り組みを開始

「情報セキュリティ基本方針」のサンプルを参考に自社の基本方針を作成。さらに「５分でできる！情報セキュリティ診断」で実施状況を把握する。

STEP３　本格的に取り組む

対応すべきリスクと対策を検討し、サンプルを参考に自社のリスクに応じた規定を定める。

STEP４　より強固にするための方策

「クラウドセキュリティ」など自社に必要な対策や「セキュリティインシデント」発生時に必要な対策を実施する。

「リスク分析シート」を活用した詳細リスク分析を実施する。

ガイドラインの実践編を参考に自社にあったSTEPから進めてください。
経営者の方は経営者編をご覧ください。

【STEP１】できるところから始める

⑴情報セキュリティ５か条

「情報セキュリティ５か条」は、組織の規模を問わず必ず実行していただきたい重要な対策を５か条にまとめ説明したもの。対策は以下の通り。

①OSやソフトウェアは常に最新の状態にしよう！

OSやソフトウェアを古いまま放置していると、セキュリティ上の問題点が解決されず、それを悪用したウイルスに感染してしまう危険性がある。お使いのOSやソフトウェアには、修正プログラムを適用する、または最新版を利用するようにする。

【対策例】

・WindowsUpdate、（WindowsOSの場合）、ソフトウェア・アップデート（macOSの場合）などベンダの提供するサービスを実行する。
・Adobe Reader、ブラウザなど利用中のソフトウェアを最新版にする。
・テレワークで利用するパソコン等のソフトウェアやルーター等のファームウェアを最新版にする。
・利用中のソフトウェアに脆弱性が存在しないか、MyJVN バージョンチェッカ（https://jvndb.jvn.jp/apis/myjvn/vccheckdotnet.html）で確認する。

②ウイルス対策ソフトを導入しよう！

ID・パスワードを盗んだり、遠隔操作を行ったり、ファイルを勝手に暗号化するウイルスが増えている。ウイルス対策ソフトを導入し、ウイルス定義ファイル（パターンファイル）は常に最新の状態になるようにする。

【対策例】

・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の導入を検討する。
・OSに標準搭載されているセキュリティ機能を有効活用する。
・テレワークで利用するパソコン等の端末にウイルス対策ソフトを導入し、ウイルス定義ファイルを最新

の状態にする。
③パスワードを強化しよう！
パスワードが推測や解析されたり、ウェブサービスから流出したID・パスワードが悪用されたりすることで、不正にログインされる被害が増えている。パスワードは「長く」、「複雑に」、「使い回さない」ようにして強化が必要。
【対策例】
・パスワードは10文字以上で「できるだけ長く」、大文字、小文字、数字、記号含めて「複雑に」、名前、電話番号、誕生日、簡単な英単語などは使わず、推測できないようにする。
・同じID・パスワードを複数サービス間で使い回さない。
・テレワークでVPNやクラウドサービスを利用する際は、強固なパスワードを設定し、可能な場合は多段階認証や多要素認証を利用する。
④共有設定を見直そう！
データ保管などのウェブサービスやネットワーク接続した複合機の設定を間違ったために、無関係な人に情報を覗き見られるトラブルが増えている。無関係な人が、ウェブサービスや機器を使うことができるような設定になっていないことを確認する。
【対策例】
・ウェブサービス、ネットワーク接続の複合機・カメラ、ハードディスク（NAS）などの共有範囲を限定する。
・従業員の異動や退職時には速やかに設定を変更（削除）する。
・テレワークで使用するパソコン等は他者と共有しない。共有せざるを得ない場合は、別途ユーザーアカウントを作成する。
・外出先でフリーWi-Fiを使うときにはパソコンのファイル共有をオフにする。
⑤脅威や攻撃の手口を知ろう！
取引先や関係者と偽ってウイルス付のメールを送ってきたり、正規のウェブサイトに似せた偽サイトを立ち上げてID・パスワードを盗もうとする巧妙な手口が増えている。脅威や攻撃の手口を知って対策をとる。
【対策例】
・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。
・テレワークでは管理者が従業員に適宜注意喚起し、従業員はセキュリティの懸念は速やかに報告する。

【STEP２】組織的な取り組みを開始する

⑴情報セキュリティ基本方針

「情報セキュリティに関する基本方針」は、情報セキュリティ対策を組織的に実施する意思を、従業員や関係者に明確に示すために、どのような情報をどのように守るかなどについて、自社に適した方針を定めるもの。
業務や顧客の期待の変化なども踏まえて基本方針なども適宜見直しを行うことが必要。
基本方針には、決まった書き方はないので、「情報セキュリティ基本方針（サンプル）（中小企業のセキュリティ対策ガイドライン付録２）」を参考にして、事業の特徴や顧客の期待などを考慮したうえで経営者と連携しつつ、自社に適した基本方針を作成する。
また、基本方針は従業員の指針であり、関係者に対して取り組みを表明するためのものなので、作成した文書は、従業員や顧客などの関係者に周知する。
〇情報セキュリティ基本方針の記載項目（例）
・管理体制の整備　・法令・ガイドライン等の順守
・セキュリティ対策の実施　・継続的改善　など

⑵５分でできる！情報セキュリティ自社診断

「５分でできる！情報セキュリティ自社診断」は、情報セキュリティ対策のレベルを数値化し、問題点を見つけるためのツールである。
同診断は、独立行政法人情報処理推進機構セキュリティセンターのHP（https://www.ipa.go.jp/security/guide/sme/５minutes.html）に掲載している。
診断編を利用することにより、情報セキュリティ対策の現状を把握することができる。さらに、解説編では、各チェック項目で設定されている設問についての解説がある。この解説編を参照することで、診断編にある設問の内容を自社で対応していない場合に生じる情報セキュリティへのリスクと、今後どのような対策を設けるべきかを把握することができる。
①診断編
25個の診断項目に答えると、自社の情報セキュリティの問題を簡単にチェックできる。
〇診断内容
ウィルス対策、パスワード管理、Web利用のルール、無線LANのルール、情報の安全な処分、取引先管理、私物機器の利用等
②解説編
診断編で問題のあった項目は、解説編を見て対策を検討する。解説編には、対策を立てる上での考え方や具体的な対策例が紹介されている。
③対策の決定と周知
診断結果をもとに、解説編を参考にして実行すべき情報セキュリティ対策を検討する。自社診断には、あまり費用をかけず、効果があると考えられる対策例が示されているので、診断結果に基づき、実施すべき対策を検討する。具体的な使い方は以下のとおり。
・対策の検討と決定は、責任者・担当者と経営者が行う。
・診断項目ごとに対策を実施しない場合に考えられる被害・事故や、防止するための対策例が示されているので、参考にして検討する。
・対策を検討するときには従業員の意見を聞き、職場環境や業務に適した対策を決定する。

【STEP３】本格的に取り組む

⑴情報セキュリティ規程の作成

企業を取り巻くリスクは、事業内容や取り扱う情報、職場環境、ＩＴの利用状況などによっても異なることがあり、汎用的な規程をそのまま使っても、自社に適さないことが考えられる。効率的に自社に適した規程を作成する方法は以下のとおり。

①対応すべきリスクの特定
　経営者が懸念する情報セキュリティの重大事故などを念頭に、何が起こらないようにするべきかを考える。この時、以下のような状況を併せて考えることで、対応すべきリスクを把握する。
・関連する業務や情報に係る外部状況（法律や規制、情報セキュリティ事故の傾向、取引先からの情報セキュリティに関する要求事項など）
・内部状況（経営方針・情報セキュリティ方針、管理体制、情報システムの利用状況など）
②対策の決定
　全てのリスクに対応しようとすると、費用が多額になったり、仕事が非効率になったりすることがある。そこで、いつ事故が起きてもおかしくない、あるいは事故が起きると大きな被害になるなど、リスクが大きなものを優先して対策を実施し、事故が起きる可能性が小さいか、発生しても被害が軽微であるなど、リスクが小さなものについては、現状のままにするなど、合理的に対応する。
③規程の作成
　②で決定した対策を文書化した規程を作成する。「情報セキュリティ関連規程（サンプル）」（https://www.ipa.go.jp/security/guide/sme/about.html）のサンプル文中の赤字、青字部分を自社向けに書き換えれば、規程が完成する。なお、サンプルに明記されていなくても必要な対策や有効な対策があれば、追記を行う。

	名　称	概　要
1	組織的対策	情報セキュリティのための管理体制の構築や点検、情報共有などのルールを定める。
2	人的対策	取締役及び従業員の責務や教育、人材育成などのルールを定める。
3	情報資産管理	情報資産の管理や持ち出し方法、バックアップ、破棄などのルールを定める。
4	アクセス制御及び認証	情報資産に対するアクセス制御方針や認証のルールを定める。
5	物理的対策	セキュリティを保つべきオフィス、部屋及び施設などの領域設定や領域内での注意事項などのルールを定める。
6	ＩＴ機器利用	ＩＴ機器やソフトウェアの利用などのルールを定める。
7	ＩＴ基盤運用管理	サーバーやネットワーク等のＩＴインフラに関するルールを定めます。
8	システム開発及び保守	独自に開発及び保守を行う情報システムに関するルールを定めます。
9	委託管理	業務委託にあたっての選定や契約、評価のルールを定める。委託先チェックリストのサンプル付属。
10	情報セキュリティインシデント対応ならびに事業継続管理	情報セキュリティに関する事故対応や事業継続管理などのルールを定める。
11	テレワークにおける対策	テレワークのセキュリティ対策についてルールを定める。

【STEP４】より強固にするための方策
　ＩＴの普及に伴い情報セキュリティ対策も重要視されている。技術の悪用や技術的な攻撃を防ぐためには、人的な注意や対策だけでは限界があり、技術的対策を強化したり、外部の専門サービスを利用する必要がある。
　事業でコンピュータやインターネットを活用している企業が、より強固な情報セキュリティ対策に取り組むために必要とされる以下の技術的対策や、対策の導き出し方などを「中小企業の情報セキュリティ対策ガイドライン第3.1版」の32Pで解説している。詳細は同ガイドライン参照。

Ⅲ．相談窓口

１．サイバー事案に関する相談

①サイバー事案に関する通報等のオンライン受付窓口（警察庁）
　警察庁では、サイバー事案に関する通報、相談及び情報提供の全国統一のオンライン受付窓口（https://www.npa.go.jp/bureau/cyber/soudan.html）を設置している。
　同窓口からはサイバー事案に関する以下を行うことができる。
・通報（都道府県警察に対し、サイバー事案に関する通報を行うもの。）
　※被害に遭った具体的な事実の通知を伴う場合
・相談（都道府県警察に対し、サイバー事案に関するアドバイスを求めるもの。）
・情報提供（都道府県警察に対し、サイバー事案に関する情報を提供するもの。）
　この窓口から通報等を行う際、お住まいの都道府県の警察本部や管轄警察署を選択する。通報等の内容は選択した都道府県警察本部又は警察署に通知される。
②警察署に来署
　警察署に来署し相談する際は、担当者不在の場合があるため、住所地を管轄する警察署（茨城には27箇所）にあらかじめ電話連絡をし、日程調整を行ってから来署相談を行う。

２．情報セキュリティ対策に向けた専門家への相談

　中小企業庁が各都道府県に設置した無料の経営相談所である「よろず支援拠点」では、専門家から情報セキュリティに関するアドバイスを受けることができる。
〇問い合わせ先
　TEL：029-224-5339　FAX：029-227-2586
　mail：yorozu@iis-net.or.jp