サクセスネット SuccessNet

中小企業の経営者が知っておきたい

サイバーセキュリティ対策

資料作成：特定社会保険労務士　堀川 眞也

目次

中小企業の経営者が知っておきたい

サイバーセキュリティ対策

■１．サイバー攻撃とは

（１）業務効率化のための IT 機器

いまや、パソコン、スマートフォン、インターネット(以下「IT 機器」とします)を利用せずに業務を行うことは考えられず、それら IT 機器をツールとして使う事で業務を効率的におこなう事ができます。

IT 機器以外にも業務で用いるツールには様々ありますが、誤った使い方をすると逆にダメージを受けることになります。

例えば、自動車。とても便利ですが、事故は避けたいものです。

製品製造のための機器も安く大量に生産するには必要ですが、場合によっては巻き込まれ事故などが発生することもあります。

IT 機器なども業務を効率化するためには必須ですが、その使い方を誤れば、情報漏えいや、サイバー攻撃の的となり、業務停止や、損害賠償の責任を負うような事にもなりかねません。

IT 機器を正しく使用し、サイバー攻撃から会社を守ることはこれからの業務を行っていく上で大変重要になってきます。

（２）サイバー攻撃とは

サイバー攻撃とは、インターネットや IT 機器を用い、個人や組織を対象に、金銭の窃取や個人情報の詐取、あるいはシステムの機能停止などを目的として行われる攻撃です。例えば以下の様な目的があります。

１．不正アクセスにより企業が保有する機密情報や顧客情報を窃取する
２．ホームページやシステムをダウンさせるなどして何かしらの被害を与える
３．ID やパスワードを入手し、不正ログインやなりすましによるクレジットカードの不正利用、預金口座から送金する

（３）サイバー攻撃の目的

サイバー攻撃を行う目的はさまざまです。

１．愉快犯的な犯行や自身が持つ技術力を見せつけたいというもの
２．金銭の収奪を目的とするもの
３．特定組織の機密情報を窃取するもの
４．企業活動の停止を目的とするもの
５．ある特定の相手を攻撃するための踏み台としてパソコン等を乗っ取るもの

いずれにしても、ひとたび攻撃に遭ってしまえば、企業活動に様々な影響があり、場合によっては企業存続の危機に陥ることになります。

（４）セキュリティインシデントの発生状況

IPA 情報処理推進機構発行の「情報セキュリティ白書 2022」によれば、国内の 2021 年のセキュリティインシデントの発生状況は 769 件となり、2020 年の 537 件から 43%増加しています。毎日 2 件程度、情報セキュリティ事故が発生していることになります。

また、割合が最も多いのは「不正アクセス」で、37.2% でした。

前年比では、「不正アクセス」が 141.6%、「改ざん」が 242.9%、「情報流出」が 135.6%、「その他」が 129.9% でした。

https://www.ipa.go.jp/security/publications/hakusyo/2022.html

（５）サイバー攻撃の種類

主なものについて説明します。

◎ウイルス、不正プログラム

ウイルス、不正プログラムがパソコンに感染することにより、情報の搾取や、パソコンの機能停止、他のパソコンを攻撃するための踏み台などにされてしまいます。

ウイルスの感染経路には主に以下の 4 つがあります。

①　電子メールによる標準型攻撃

電子メールにウイルスを仕込んだファイルを添付し、それを開封することで、ウイルスに感染させ、パソコン内や社内ネットワーク上の情報の搾取や、そのパソコンから、さらにウイルスをばらまくメールを送信してしまうなどを行う。

②　記憶媒体からの感染

ウイルスに感染した USB メモリーや、外付けハードディスクなどをパソコンに接続するだけで、そのパソコンにウイルスが感染する

③　インターネットによる感染

ウイルスが仕掛けられたページを閲覧するだけで感染する(アダルトサイトからの感染など)

また、パソコンの Windows OS や、ソフトウエアの脆弱性から侵入するケ

ースもあり。

④　ネットワークによる感染

1台のパソコンが感染することにより、社内ネットワークに接続されたパソコンに次々と感染してしまうケース。

これらウイルス、不正プログラムによる感染で有名なのは、Emotetという、メール添付型の不正プログラムや、ランサムウェアというパソコンを暗号化する不正プログラムで、この不正プログラムに感染させることにより、パソコンを使えなくした上で、元に戻すことと引き換えに金銭などを要求(身代金要求)されます。最近では、病院の電子カルテを使えなくし、病院の診療停止に追い込むなどの事件が発生しています。

◎フィッシング

フィッシングとは、実在する有名企業を装って電子メールを送信し、偽のWebサイトに接続させることで、クレジットカード番号やID、パスワードなどの個人情報を窃取します。偽の通販サイト、宅配業者、銀行などになりすましたメールが送られてくるのが特徴です。

例えば、メール本文に書かれている、URLをクリックすることで、偽サイトにアクセスさせ、IDとパスワードを入力させ、それらを盗み取るものです。

◎サプライチェーン攻撃

上記の他、大企業の情報を搾取する目的で、比較的セキュリティ対策が手薄な関係取引先の中小企業を狙い、その中小企業を経由し、大企業の情報を盗み出すものです。

◎その他の攻撃

★SQLインジェクション:

アプリケーションの脆弱性を攻撃し、個人情報の漏洩、Webページの改ざんを狙うもの。

★DDoS攻撃：

攻撃対象となるWebサーバーなどに対し、複数のコンピューターから大量のパケットを送りつけることで、正常なサービス提供を妨げるもの。

★ブルートフォースアタック：

総当たり攻撃ともいう。暗号の解読やパスワードの割り出しなどに用いられる手法の一つで、割り出したい秘密の情報について、考えられるすべてのパターンをリストアップし、片っ端から検証する方式。“brute force” は「力づく」の意。

■２．サイバー攻撃を受けた時のリスク

サイバー攻撃を受け、情報漏えいなどの事故を発生させた場合、以下の様な問題が発生し、企業活動が停止に追い込まれ、最悪廃業ということにもなりかねません。

大きくは以下の 4 種類に分類されます。

（１）金銭の損失

・取引先からの損害賠償、不正アクセスによる不正送金など

・業務停止による売上の減少

情報漏えい事故を発生させた企業や、個人が責任を負うことになり、被害を受けた、取引先や顧客から損害賠償を求められることになります。

2018 年度の情報セキュリティ事故 1 件あたりの平均想定損害賠償額は約 6 億円となっており、企業規模にもよりますが、情報漏えい事故は甚大な責任を負うことになります。(特定非営利活動法人日本セキュリティ・ネットワーク協会(JSNA)発行「情報セキュリティインシデントに関する調査報告書 2018」より)

例え、原因が保守業者や、従業員個人であってもまずは、会社の名前が表に出てしまいますので、第一次の責任を問われることは避けられないでしょう。

（２）顧客の喪失

・管理責任を問われ直接の関与先から契約解除

・直接関係のないお客様からも契約解除で全顧客を喪失するリスク

社会的評価の低下、風評被害などから、顧客の流出、取引の停止など企業活動停止に追い込まれ、一度失った信頼を回復するには多大な努力と時間が必要になります。

（３）業務の停滞

・被害調査、改善実施、復旧まで業務停止

・再発の防止、再教育の開始

問題の対策、再発防止策の導入など、業務停止期間が長引くことで、納期遅れ、営業機会損失、対応費用の発生、従業員に対する再教育など、長い時間正常な業務ができない事が想定されます。

（４）従業員への影響

・スタッフのモラルの低下、復旧作業によるモチベーションの低下

・最終的には離職に至る

対外的な対応、再発防止策の検討その他本来の業務ではなく、復旧に向けた

作業が続くことが想定されます。その事により、長時間労働や会社の将来性の不安から、人材の流出が避けられないことが想定されます。

これらリスクから経済的な損失をカバーするため、サイバーセキュリティ保険があります。サイバーセキュリティ保険は、サイバー事故により企業に生じた第三者に対する「損害賠償責任」のほか、事故時に必要となる「費用」や自社の「喪失利益」を包括的に補償する保険です。

経済的な損失から会社を守る為に加入の検討も必要です。但し、失った信頼の回復は時間がかかります。まずはサイバーセキュリティ事故を発生させないことが重要です。

■３．サイバー攻撃を受けて事故が発生した場合の対応策

サイバー攻撃を受けたかもしれない、若しくは受けてしまったことが明らかになった場合、早急な対策を行い、被害の拡大の防止を行う必要があります。

そのまま放置すると、被害が大きくなり収拾の困難さが増してきます。

（１）報告体制

・サイバー攻撃が起きたときのための BCP プランをあらかじめ策定しておきましょう。起きたときに慌てないため、有事の対応策を決めておくことが重要です。

・サイバー攻撃を受けたかもしれない、若しくは受けてしまったことが明らかになった場合に、それに気づいた従業員が社内の誰に報告すべきなのか、あらかじめ明確にしておくことが重要です。また、報告を受けた者はすぐに対応する為の作業に取りかかることが必要で、経営者、経営幹部も巻き込み対策を開始します。

・社内にネットワーク、サイバーセキュリティに詳しい人が居ない場合、外部業者を使用することも検討してください。

（２）対策の開始

・サイバー攻撃の種類により、対策方法は様々です。主な対策方法は以下の通りです。

①　ウイルスの感染

ウイルスに感染したと思われるパソコン等は、直ちに社内のネットワークから切り離します。無線 LAN にも接続しないようにしてください。

ウイルスを完全除去するまでは、ネットワークから隔離を行います。

市販のウイルスソフトで、ウイルスチェックをして除去を試みます。ただしウイルスの除去ができない場合は専門家に除去を依頼することになります。

Emotet の場合、感染確認と、感染後の除去方法が以下の警視庁サイトから確認する事が出来ます。

https://www.keishicho.metro.tokyo.lg.jp/kurashi/cyber/CS_ad.files/EmoCheck.pdf

② ランサムウエア

ランサムウエアに感染した場合、対策方法は限られています。くれぐれも身代金要求に応じたり、相手先の連絡先に連絡を取ったりせず、IPA 情報処理推進機構、または警察の「サイバー犯罪相談窓口」に連絡し指示を仰いでください。

https://www.ipa.go.jp/security/anshin/ransom_tokusetsu.html

https://www.npa.go.jp/cyber/soudan.html

③ フィッシング

フィッシングにあってしまった場合は、早急にそのサイトのパスワードを変更し、盗まれた ID とパスワードを不正使用者が使用できないようにしてください。

（３）外部への影響の確認

・顧客及び取引先、関係関与先へ、影響がなかったか確認を行い、情報漏えい等の事実があった場合には、被害情報の公開や、個人情報保護委員会への報告の義務があります。

■４．サイバー攻撃を受けないための対応策や訓練

サイバー攻撃で最も脆弱性のあるのは、操作を行う人です。そして、サイバー攻撃を防ぐのも人です。その為には、IT 機器の操作についてしっかりと理解しておくことが必要です。

（１）ウイルスや不正プログラムの感染を防ぐ

① メール

知り合いから送られてきたメール、若しくは自分に関係ありそうなタイトルのメールも疑ってかかる必要があります。

a）添付ファイルをやみくもに開かない
b）タイトルを見て疑わしさを確認する
c）本文を確認し、日本語が正しいかどうか、必要な内容か見きわめる
d）送信者に送付の事実を確認する
e）本文の URL は絶対にクリックしない

メールからの感染を防ぐのは、メールを受信する担当者自身にかかってい

ます。絶対に騙されない為にも、注意に注意を払ってメールを開いてください。

② 外部装置からの感染を防ぐ

a）USB メモリー、外部記憶装置は使わない、使わせない

b）データの送付、交換は信頼できるサーバーを経由すること

③ 脆弱性対策

a）サポート期限の切れた OS やソフトを使わない

（ア）Windows は、10 または 11 のみ使用する事（7 や、8.1 は使用しない）

（イ）MS Office は 2016 以降のものを使用すること （2013 以前のものは使用しない）

b）「更新してシャットダウン」が出た時は、必ず行う

④ 業務用パソコンで、私用のネット接続を禁止する

業務用パソコンは業務を行うためのものです。私用のネット接続でウイルスに感染するリスクが高まります。私用のネット接続は禁止しておく事を従業員に熟知させる事が必要です。

⑤ 私用のパソコン等（個人所有の）を業務で使用しない。

社内のネットワークに接続させない。

（２）フィッシングを防止する

メール本文の URL リンクをクリックすることで、偽のサイトに接続してしまい、ID やパスワードが盗まれる事案が多く発生しています。

フィッシング被害を防止するには、メール本文の URL リンクをクリックせずに、面倒でもブラウザ（インターネットを見るためのソフト Edge や、Chrome）から関連のサイトにアクセスしてください。

例えば、通販サイトの支払に関するメールが届いたとき、メール本文の URL をクリックせず、ブラウザを立ち上げ、その通販サイトへ接続し、ご自身の支払に関する情報を確認してください。

（３）ウイルス除去ソフトの導入と有効化

Windows10 以降は、Defender という、ウイルス除去ソフトが導入されていますが、動作をオフにしていたり、「更新してシャットダウン」をしていないと正常に動作をしなくなります。また、市販のウイルスソフトを導入している場合も、アップデートを怠っていたり、期限切れなどで動作が停止している場合もあります。

ウイルス除去ソフトを正常に動作させるために、利用者任せではなく、会社として一律に確認することをお勧めします。

企業の規模が大きくなれば、サーバー管理型の業務用セキュリティソフトの導入も検討してください。

（４）パスワードの強化

パスワードは使い回しをせず、必ず違うパスワードを使用してください。
ご自身でパスワードのパターンを決めておくと覚えやすくなります。
また必ず８文字以上、大文字、小文字、数字、記号を混ぜておきましょう。
（例）〇〇〇XXXXXX　　XXXXXX の部分はすべて共通として、〇〇〇の部部分について、サイト毎に変えておくなど。

（５）現状掌握、訓練と教育

①　現状掌握

偽のフィッシングメールや、偽ウイルスを仕込んだメールをスタッフに送信し、どのくらいの人が、騙されて開いてしまうかを確認する訓練メールを行うサービスがあります。

②　対応訓練

実際に有事の際にどのように対処するか、避難訓練と同様、年に１度程度訓練をおこなう事も有効です。

③　教育

サイバー攻撃は、進化を続けており、新しい攻撃方法が次々に生まれています。常に緊張感を持って IT 機器に接するためにも継続した教育が必要です。

IPA 情報処理推進機構等が発行している、チェックリストや資料など用い常に情報のアップデートを行う事が重要です。

以下の「5 分でできる診断シート」等も参考にしてください。

https://www.ipa.go.jp/files/000055848.pdf

5 分でできる診断シート

https://www.ipa.go.jp/security/keihatsu/sme/guideline/5minutes.html

5 分でできる診断解説

④　セキュリティポリシー、規程の作成

セキュリティポリシーとは、セキュリティ対策について定めた基本方針のことです。セキュリティポリシーを明確に設定することで、従業員は行っても良い行動と悪い行動が理解出来るようになります。また、社内の情報セキュリティについて、規程として文章化し、従業員全員の責任と責務、対応について明確にすることで、セキュリティ事故のリスクを下げることが可能です。

■５．まとめ

サイバー攻撃等による情報セキュリティ事故は、自社のみならず、関係先関与先まで影響を与え、企業の存続にかかわる問題にまで発展します。

しかしながら、最もサイバー攻撃に弱いのは、IT 機器を操作する人であり、漫然と IT 機器を使用する事が会社を危険にさらす事になりかねません。まさに情報セキュリティ事故は、「人災」と言っても過言ではありません。

定期的な教育・訓練を積み重ね、従業員一人ひとりがその重要性を理解し、緊張感を持って、IT 機器を利用することが求められています。是非ともサイバー攻撃から会社を守り、自社から情報セキュリティ事故を発生させないように努めましょう。

IT に関しては専門家もいない、何から手をつけていいかわからないと言うこともありますが、まずは IPA が推奨する「情報セキュリティ５ヶ条」からはじめてみてください。

１．OS やソフトウェアは常に最新状態にしよう！
２．ウイルス対策ソフトを導入しよう！
３．パスワードを強化しよう！
４．共有設定を見直そう！
５．脅威や攻撃の手口を知ろう！

https://www.ipa.go.jp/files/000055516.pdf

そして、以下の操作の前に一呼吸入れて、サイバー攻撃から身を守ってください。

１．メールを開く前に
２．添付ファイルを開く前に
３．URL をクリックする前に
４．USB を挿す前に
５．SMS を見る前に

【著者プロフィール】堀川 眞也（ほりかわ しんや）
社会保険労務士事務所 フェリシアンス® 代表
株式会社フェリシアンス® 代表取締役
特定社会保険労務士・キャリアコンサルタント
IPA 情報処理機構セキュリティプレゼンター

外資系、日系の IT 機器メーカー３社で、３２年の会社員を経験した後、2017 年社会保険労務士事務所を開業。

キャリアコンサルタント＋社労士として、「従業員も経営者もずっとハッピー」を目指すコンサルティングや、就労支援のためのセミナーを行っています。

外資系会社員時代、機密情報の保管、保持、パソコンに於ける情報漏えいの防止について厳しい教育訓練を受けた経験から、情報を守るべき現場の立場で、セキュリティについてわかりやすく解説をしています。