The title 2

浅間商事株式会社
代表取締役社長
柳沢 太一
URL　https://www.asama-shoji.co.jp/
公式 YouTube　https://www.YouTube.com/@user-zh5er1ix6p

今すぐ始める中小企業の情報セキュリティ基本対策術

「旧知の企業がサイバー攻撃を受けたらしい。ウチは大丈夫だろうか？」「取引先から情報セキュリティ対策の強化を求められたが、どこから手を付けていいのかわからない…」これは、弊社のクライアントから寄せられた悩み事です。そこで、中小企業がローコストで始められる情報セキュリティ対策術を本稿で紹介します。

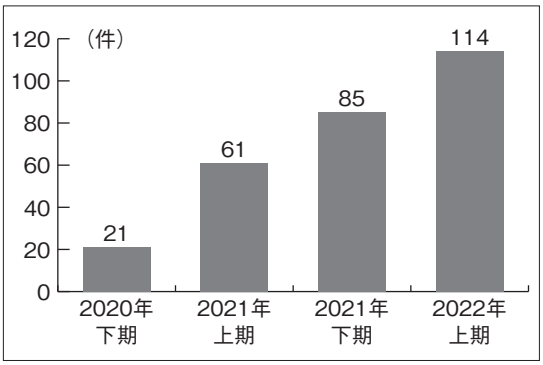
中小企業へのサイバー攻撃事例

「サイバー攻撃なんてSFの話…」と思っていた方が、実際、ご自身や身近な人が被害に遭ったことで、はじめて社会問題として認識したケースは少なくありません。

サイバー攻撃のひとつ「ランサムウェア」（データを暗号化などにより利用不可能にして、身代金を要求するウイルス）による被害件数は2020年の下半期以降、急増しています。企業・団体が被害を受けたとして警察庁に報告があった件数を見ても、2021年上半期の61件に対して2022年上半期には114件と、1年間でおよそ2倍に増加しています（図1／警察庁2022年4月公開）。

では、サイバー攻撃とは一体どのようなものなのでしょうか。まずは、弊社が入手した被害事例2つを以下に掲載します。

図1　ランサムウェア被害の報告件数（企業・団体等）



出典：警察庁 Web サイト

事例①：A 社（小売業 / 従業員数：約 30 名）

社内システムがランサムウェアに感染し、基幹サーバーのデータおよびバックアップ用ハードディスク内のデータが消失。早期の事業復旧を優先するため、身代金として数千万円を支払って暗号化を解除した。

事例②：B 社（小売業 / 従業員数：約 200 名）

国内 10 拠点、合計 200 台のパソコンが VPN（仮想プライベートネットワーク）を通じてランサムウェアに感染し、暗号化された。本社サーバーおよび、バックアップ用の NAS（ネットワーク接続ハードディスク）もすべて感染し業務が停止。復旧業者に依頼して、約 1,500 万円の費用と 1 ヶ月の時間を費やして業務を復旧させた。

この2件の事例と同様に、最近はランサムウェアによる被害が目立ちます。身代金の支払額も以前は数十万円程度に留まっていたケースが、ここ数年、数千万～数億円規模に高騰しています。

セキュリティ対策は中小企業でも必要なのか？

サイバー攻撃を受ける企業・団体は業種も規模も様々です。IT技術の発展により大量のウイルスをばらまくことが容易になった現在、サイバー攻撃を実行する犯罪グループは個人も中小企業も大企業も区別せず、無差別に攻撃をしかけています。それが、たまたま防御に穴が開いているサーバーなどに届くと感染してしまいます。

特許や技術情報、高額の身代金を目当てに特定の企業・団体を狙い撃ちする場合もありますが、私たち中小企業が警戒すべきは無差別攻撃です。サイバー攻撃の流れ弾から会社を守るためには、業種や規模にかかわらず、最低限の対策を講じる必要があります。

では、中小企業が最低限やっておくべきセキュリティ対策とはどのようなものでしょうか。

それは、大きく分けると、

「情報を知る」
「システムを導入する」

この2つになります。

情報を知ることは直ちに、そして費用をかけずにできます。常に最新の情報を知り日々気を付けることがセキュリティ対策の第1歩ですが、人間が気を付けられることには限界があります。より精度の高い対策のためには、それを補うシステムの導入が必要です。

中小企業がやるべきセキュリティ対策 その1

「情報を知る」

情報を知る必要があるのは、経営者や情報システム担当者だけではありません。全社員が適切な情報を確知することで、会社全体のセキュリティ意識の向上を図ります。以下に、全社員に知ってほしい「7つのセキュリティ対策」（①～⑦）を紹介します。

①パスワード管理

●長く複雑なパスワードにする、使い回さない、共有しない

パスワードは、長く複雑なものを設定します。可能な限り長めで、さらに、英字（大文字・小文字）・数字・記号を複雑に組み合わせることをオススメします。辞書に載っているような推測されやすい単語、家族の名前や生年月日、電話番号などは避けてください。

また、異なるサービスで同一のパスワードを使い回すのは危険です。もしも、ひとつのサービスからパスワードが漏えいした際には、他のサービスにも侵入される恐れがあります。

②アップデート

●OSやブラウザ、ソフトをアップデートする

PCのOSやソフトには、サイバー攻撃の原因になる弱点（脆弱性）が見つかることがあります。その弱点を修復するのがアップデートです。基本的には、通知が来たらできるだけ早くアップデートしてください。しばらく起動していないパソコンなどは、まずは利用する前にアップデートを実施します。

③メール

●あやしいURLや添付ファイルは開かない

身に覚えがないメールはもちろん、取引先からのメールでもなりすましの可能性があります。少しでもあやしいと感じたら、URLや添付ファイルは安易にクリックしないで、まずはメール以外の方法で送信元に確認を取ります。

URLを開いたことで不正なサイトにアクセスしてしまったり、偽サイト（フィッシングサイト）で入力したIDやパスワードを窃取されたりしてしまう危険性があります。また、ウイルスが仕込まれた添付ファイルを開いてしまう

と感染する場合があるので注意が必要です。

④バックアップ
●大切なデータは複数のバックアップを取る

近年、増加しているランサムウェアは、データを暗号化して使えないようにして身代金を要求する手口です。万が一、暗号化されてしまっても正常なバックアップがあればデータを迅速に復元できます。

データのバックアップは、ファイルを誤って削除や上書きしてしまった場合など日常的に発生する誤操作や、パソコンの急な故障などのトラブル時にも役立ちます。

⑤Ｗｅｂサイト
●偽サイト（フィッシングサイト）や怪しいファイルのダウンロードに注意する

偽サイトなどへのアクセスはもちろん、Ｗｅｂサイトからファイルやソフトをダウンロードする際にも注意が必要です。ウイルスが仕込まれたものを利用することで感染するケースがあります。

⑥社内外での端末・メモリ利用
●私用の端末・メモリを社内ネットワークで利用しない
●社用の端末・メモリを社外ネットワークで利用しない

ウイルスに感染した私用の端末（パソコン、スマートフォン等）やＵＳＢメモリを、気付かないまま会社のネットワークにつなげて利用すると、感染を社内に広げてしまう危険性があります。

また、会社用の端末やＵＳＢメモリを、社外の安全性が確認できないネットワークにつなぐと端末内の情報を抜き取られてしまったり、ウイルスに感染するリスクも高まります。

原則、端末やＵＳＢメモリ、接続するネットワークは私用と会社用で分けて利用します。また、外出先では端末やＵＳＢメモリから目を離さず、万が一に備えてロックやパスワード保護をかけておくことを心掛けてください。

⑦最新情報を知る
●最新かつ信頼できる情報を入手する

セキュリティ対策のための情報を得るには、まずは信頼できる情報源を見つけておくことが必要です。現在、サイバー攻撃による被害が増えているため各省庁で積極的に情報を発信しています。

その中でも、特に中小企業の方にチェックしてほしいのが、次の２つのサイトです。

・内閣サイバーセキュリティセンター（ＮＩＳＣ）
https://www.nisc.go.jp/

ＮＩＳＣはサイバーセキュリティ基本法に基づき２０１５年に内閣官房に設置された組織です。基本的なセキュリティ対策情報を提供しています。

サイト内に掲載されている「ＮＩＳＣソーシャルメディア」に登録をしておくと、最新情報が手軽に入手できるため大変便利です。こちらでは、Twitter、Facebook、LINE、YouTube が利用できます。

・SECURITY ACTION（セキュリティ対策自己宣言）
https://www.ipa.go.jp/security/security-action/index.html

経済産業省所管の機関であるＩＰＡ（独立行政法人情報処理推進機構）によって創設された、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す。本サイトでは、中小企業が初めに取り組みたい情報セキュリティ対策ガイドラインを提供しています。

ガイドラインに従い対策を実施する企業は「SECURITY ACTION」のロゴマークの使用を申請できます。ロゴマークを活用することで取引先や金融機関に対して、対策アピールや信頼度の向上が期待できます。

以上の7つが、新入社員も含めた全社員に知っておいてほしい情報です。とても基本的な対策ですが、これらを適切に把握して実施することで防げる被害も多いはずです。

中小企業がやるべきセキュリティ対策 その2

「システムを導入する」

システムを導入する際の基本的な考え方が「多層防御」です。ウイルス対策ソフトひとつで全ての攻撃は防御できません。したがって複数のものを組み合わせて防御力を高める必要があります。

弊社は、クライアントに対して以下の「3つの対策」（①～③）を推奨しています。

①ウイルス対策ソフト

Windows標準のウイルス対策ソフトもレベルが上がってきましたが、ウイルス対策の専用ソフトを導入した方がセキュリティは向上します。特にテレワークや社外での仕事が増えている現在、ウイルス対策ソフトは最後の防衛線といえます。

ウイルス対策ソフトを導入していたとしても、ライセンスが切れていたり、アップデートができていなかったりして正しく機能していない状況が散見されます。

今どきのウイルス対策ソフトは「クラウド管理」ができるようになっており、中にはWindows Updateの状況を確認・通知してくれるものもあります。

②UTM（Unified Threat Management）

UTMは「セキュリティ機能付きのルーター」のことです。インターネットに接続するためにはルーターという箱型の器機が必要になりますが、これをセキュリティ機能付きのものにすることでインターネットの出入り口を守ることができます。

最近のサイバー攻撃は、メールやホームページなどを利用したインターネットからの侵入が多く見られます。また、ウイルスが社内に入ってしまうと、社外とやり取りした際にウイルスをばらまいてしまう危険性がありますが、それを防ぐことも可能です。

加えて、サイバー攻撃されていないか、業務に不必要な活動がないかなどを監視することもできます。UTMを導入した企業の中では、業務に関係のないECサイトや動画サイトの履歴、夜勤時にはアダルトサイトの閲覧が見つかったという事例もあります。

③データのバックアップ

貴社の大切なデータはどこに保存していますか？

「パソコンの中だけ」「サーバーやNASの中だけ」では、非常に危険です。そこにウイルスが感染したり、もし機械が壊れたりしたらデータが消失してしまいます。

一般的に、バックアップは3箇所が推奨されており、それは自身のパソコン、サーバー、サーバーのバックアップです。

ただし、最近のサイバー攻撃はこれら3つすべてが暗号化されてしまう事例も増えており、3つ目のバックアップは、クラウド上や常に同期がされない設定にしたNASなどを利用することを推奨します。

④メールのフィルタリング

添付ファイルにウイルスが含まれていないか、フィッシングサイトのリンクが含まれていないかなどを、メールを受信する前に自動でチェックしてくれるシステムです。ウイルス対策ソフトの上位ライセンスやMicrosoft Exchangeなどのクラウドメールのオプションとして追加可能です。

⑤クラウドメール（メールのバックアップ）

古いメールシステムの場合、メールのデータがパソコン端末内にしか保存されず、パソコンがウイルス感染や故障をした際には全てのメールデータが失われてしまうことがあります。それを防ぐためには、メールのバックアップを取

以上の3つがシステム導入の基本ですが、最近は「Emotet」（エモテット）と呼ばれるウイルスなどの、メールからの攻撃が急増しており、次の2つ（④・⑤）も費用対効果が高く推奨します。

ることが有効です。

Microsoft Exchange などのクラウドメールを使うと、データがクラウド上に自動で保存されるため手間なくバックアップを取ることができます。

「多層防御は古い」「最近はゼロトラストが必要だ」というコメントもあります。しかし、多層防御が破られる前提で、破られたらすぐに反応するという考えに基づく「ゼロトラスト」は、コストが高く中小企業では導入が難しいのが現状です。まずは、必要最低限の「多層防御」で万一に備えることからスタートしましょう。

被害に遭ってしまった…その場合の対応策

サイバー攻撃の被害に遭ってしまった場合には、まずＬＡＮケーブルを抜く、Ｗｉ‐Ｆｉを切断するといった方法で、感染した端末をネットワークから外します。

不用意にフォーマット（初期化）やリカバリーをすると攻撃の侵入経路などの証拠が消えてしまうこともあるので、焦らず対応することが大切です。

その後は、サポートを受けている業者に早急に相談をします。サポートを受けていない場合や業者でも解決ができないときは、「ＩＰＡ情報セキュリティ安心相談窓口」や「各都道府県警察のサイバー犯罪相談窓口」などに相談してください。サイバーセキュリティ保険に加入されている場合は、保険会社の窓口にも忘れずに連絡をしてください。

ただし、被害を受けてから復旧業者を探す場合には、慌てず慎重に検討しましょう。作業内容や費用について充分な説明を聞かないまま依頼をして、高額請求されてしまうケースも増えています。

専門家であっても、詳しく調査しないと復旧の可否を判断することはできません。Ｗｅｂサイトや電話で問い合わせをしただけで「必ず復旧できます」と断定したり「早くしないと復旧の可能性が下がりますよ」などと、不安につけ込むように契約を催促したりする業者には注意が必要です。

●まとめ

サイバー攻撃が増加する今、中小企業でも情報セキュリティ対策が必須となっています。

その対策には、まず、

「情報を知る」

「システムを導入する」

ことが重要です。また、システムを導入する際には、ひとつの防御で全ては賄えないので、

「多層防御」

という考え方が大切になります。

セキュリティ対策は単なるコストではなく、チャンスでもあります。適切な対策を取ることで取引先や金融機関からの信頼度が向上し、他社との差別化や社員の安心感にもつながります。また、データのバックアップを取っておくことで、誤って削除してしまったデータをすぐに復旧させることもできるようになります。

最後に、情報セキュリティ対策状況を可視化するためのチェックリストを作りました（図２）。今すぐチェックして大きな被害に遭う前に、できるところから対策を実行してください。

図２　情報セキュリティ対策の状況可視化チェックリスト

	質　問	チェック
1	パスワードは長く複雑なパスワードを使っていますか?	
2	パスワードを使い回していませんか?	
3	パソコンのWindows Updateは最新ですか?	
4	仕事に使うスマートフォンやタブレットのOSは最新ですか?	
5	ウイルス対策ソフトのバージョンは最新ですか?	
6	UTMファームウェアのバージョンは最新ですか?	
7	データのバックアップは取っていますか?	
8	メールフィルタリング（迷惑メール対策）は行っていますか?	
9	定期的にセキュリティ対策の最新情報を入手して社内共有していますか?	
10	メールのバックアップは行っていますか?	

参考資料：警視庁　令和４年上半期におけるサイバー空間をめぐる脅威の情勢等について
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_kami_cyber_jousei.pdf