

チェックリスト付き



ウイルス対策 ガイドブック



テレワークやオンライン授業、公的手続きのオンライン化が普及する中、安全にパソコンやスマートフォンを使用するためにウイルス対策のポイントをわかりやすくまとめました！



ウイルス対策ガイドブック

有料訪問サポートシェア No1^(※)の実績を持つ当社が、
ウイルス対策についてわかりやすく解説！

※ 2019年度1万人調査：個人向けパソコン、デジタル、ネットワーク機器等訪問サポートサービスシェア
(実査委託先：楽天インサイト株式会社) <2019年4月調査>

ウイルス感染による被害



まずはパソコンやIoT機器が実際にウイルスに感染してしまった際にはどのような被害が発生するのかを解説いたします。また、自分や周りの人たちへどのような影響を及ぼす可能性があるのかを理解しておくことはとても大切です。

被害事例

会社の顧客情報が流出

業務で利用するパソコンがウイルス感染してしまった場合、感染したパソコンを踏み台に社内のネットワークへウイルスが侵入してしまいます。それにより同じネットワークに接続された機器に被害を及ぼしたり、社内の機密情報などが奪われてしまうなどの被害が発生します。

さらに、感染に気づかないまま操作するとメールを介して社外にも感染を拡大させてしまう可能性があります。

クレジットカード情報流出による高額請求

何気なく開いたメールのデータや不正サイトのURLへアクセスしたことでクレジットカードの情報が盗まれてしまう可能性があります。身に覚えのない請求で判明した頃には大量に不正利用された履歴が見つかる場合もあります。



気をつけよう！よくある感染方法一例



1. 身に覚えのないメールの添付ファイルを開いてしまった
2. 不正なサイトへアクセスしてしまった
3. 安全でないデータをダウンロードしてしまった
4. 不用意に外部メモリを接続してしまった

おそらく皆さま一度は聞いたことがあるような内容なのではないでしょうか。

しかし、「自分はそんなことはしない」と思っていませんか？なぜこのように昔から危ないと言われていても被害が止まらないのか、それは**ウイルスも時代に合わせて巧妙な手口**を利用しているからです。自分ではそんなことに引っかからないと思っている人たちでもいつの間にか被害を受けていることもあるのです！

自分でできる対策を実行！



パソコンやIoT機器を利用するにあたって特に重要なのは事前に行うウイルス対策です。事例にもあった通り、甚大な被害が発生する可能性がウイルス感染には秘められています。各自ができるウイルス対策を必ず行いましょう。

また、会社で利用している機器の場合は自分だけでなく周りの人や取引先にも影響を及ぼすことも考えられます。

以下のチェックシートを参考に、改めて一人一人がウイルス対策を意識してIoT機器を安全に利用できる環境を目指しましょう。



今すぐできる！簡易ウイルス対策チェック！

- ウイルス対策ソフトが最新の状態にアップデートされている
- メールに添付されたデータは、安全を確認してから開いている
- 送られてきたURLに無闇にそのままアクセスしない
- 配信元が不明なフリーソフトなどをダウンロードしない
- USBメモリなどは感染リスクがないか確認して接続している

チェックシートの中で守れていない項目が一つでもあればウイルス対策について改めて考える機会を設けていただくことを推奨いたします。

上記を守れば必ず安全であるということはありませんが、少しでもウイルス感染のリスクを減らしておきましょう。

プロからのワンポイントアドバイス

ウイルス対策として大切なのはウイルスに対して正しい知識を持ち、どのように対策をすべきなのかを考えておくことが大切です。

まさか自分がという油断につけこんでくるのがウイルスなので、**自分も被害に遭うかもしれないという気持ち**を忘れずに機器を利用しましょう。

もし感染してしまった際にも焦らず適切な対処を行うように心がけましょう。ウイルスの中には自分で対処できるものから専門家に依頼した方が良いものまで様々なパターンがあります。困ったときには迷わず専門家へ対処を依頼しましょう。

法人向けのポイント

法人の場合は、使うソフトを制限したり、外部メモリの接続ルールを設けるなど、社内で安全にインターネットや接続機器を利用するためのルール作りを社員教育も重要です。

また、感染を確認した場合の対処法をあらかじめ決めておき社内でも共通認識を持つておくことも大切です。



近年流行したウイルス



人間がかかってしまう季節風邪のようにパソコンのウイルスにも時期によって変動が見られます。もちろん通年で被害が発生するものもあれば、一時的に被害数が爆増するといった傾向が見られる場合もあるのでデジタル機器の流行病と言えます。

ランサムウェア(身代金要求型ウイルス)

ランサムウェアに感染すると、ファイルが次々に書き換えられ、開くことができなくなってしまう。

身代金の支払いを要求するようなメッセージが表示されるケースもよくあります。

感染したパソコンのみならず、他のパソコンのデータまで書き換えるので、二次感染には十分に注意しなくてはなりません。

法人がこのウイルスへの感染を確認した場合は甚大な被害が発生する可能性があるので特に注意が必要なウイルスと言えます。



トロイの木馬

トロイの木馬とは、ユーザーに悪意のあるプログラムではないように見せかけ、ユーザーが感染していると気づかない内に破壊活動をしたり、データを流出させたりするウイルスです。トロイの木馬への感染にはさまざまなパターンがありますが、基本はどのパターンもプログラムのダウンロードとインストールを実行する点では同じです。

注意深く警戒していれば感染確率は下がりますが、勝手にダウンロード・インストールするタイプもあるため油断はできません。

エモテット

マクロウイルスというWordやExcelのマクロ機能を悪用して感染するウイルスで特に被害が広がっているのがエモテットです。感染源のパソコンからメールアドレスやアカウント情報を盗み出し、機器の中にあるアドレス帳から使用者を装ったメールでさらに感染を拡大させようとする悪質なウイルスです。

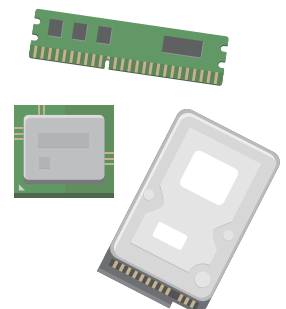
このエモテットを介して様々なウイルスに感染してしまう可能性を含んでおり感染先に合わせて変化するという特性があります。

特に近年被害が増えていることから、自宅でのパソコンの利用でも会社内での利用でも注意が必要です。

最近では特殊な事例も話題に

ウイルスはインターネットを介して機器感染させていくものが一般的です。しかし、昨今話題になっているのがパソコンの部品にウイルスが潜伏しているものです。機器がインターネットに接続されることでウイルスに感染してしまうといった内部からの感染パターンが世界では発生しています。

信頼できるメーカーや購入店を基本的に利用していただき、不明情報が多かったり怪しい内容の記載があるようなところでは機器を購入しないように心がけましょう。



ウイルスに感染した場合の対処



STEP 01

まずウイルスへの感染が疑われた場合はネットワークからの切り離しを速やかに行ってください。

情報が盗まれてしまったり大量のデータが送付されてくるといった被害が発生する前にネットワークから切り離すことができれば被害を抑えることができる可能性もあるので即座に対応しましょう。

STEP 02

もし同一ネットワークに複数の機器利用がある場合はそのほかの機器でも影響が出ていないかを即座に確認しましょう。

STEP 03

ウイルスを駆除できる場合は対応しましょう。
ウイルス対策ソフトのスキャンで特定・対処が可能であれば実施します。

改善しない場合や自身での対応が難しい場合は専門業者に依頼しましょう。

完全に初期化することでウイルスへ対応することも可能ですが、中にある資料やメールのデータも消えてしまうため、もしデータを取り出したいという希望がある場合は専門業者に依頼をいただくことで安全に対応できるので検討いただくことをお勧めします。

個人向け対策も・法人向け対策もお任せください！

当社はパソコンやIoT機器のトラブル解決を全国で対応しています。これまでウイルス対策や駆除を多数行ってまいりました。昨今は大手企業や個人を問わず誰もがインターネットやメールを使う機会があることから、ウイルスに対して正しい知識を持たなければ危険も多く存在します。

特に仕事で利用しているパソコンやスマートフォンでは在宅勤務も増えたことで、安全対策の意識が一人一人に求められます。

当社はIoTの総合サポートを行う企業としてトラブル解決だけでなく、一般のご家庭・法人それぞれの視点からウイルスの感染対策を提案・推奨いたします。「社内に詳しい人がいない」、「自宅の環境が安全かわからず不安」という方は是非ご相談ください。

ウイルス対策や、ウイルス感染に関するご相談はこちら

個人のお客さま <https://www.4900.co.jp/service/virus.php>

法人のお客さま <https://www.j-pcs.jp/business/>

会社概要

商号 日本PCサービス株式会社
代表者 家喜 信行
本社 大阪府吹田市広芝町9-33
設立 2001年9月
資本金 8月
URL <https://www.j-pcs.jp/>



セントレックス
Centrex

証券コード 6025