ウイルスに感染してしまったら・・・

- 電源を落とさずに、有線LANならケーブルを抜き、無線LANならWi-Fiを切って、ネットワークから隔離しましょう。
- すぐに社内のセキュリティ担当者へ連絡し、ウイルスを駆除しましょう。バックドアを仕掛けられていることもあるのでパソコンの初期化をおすすめします。
- 他のパソコンの感染状況も確認しましょう。

もしものためのバックアップ

- ウイルス感染によるデータの破損を想定して、数世代のバックアップ（最終版のデータだけでなく、何回か前のデータ）を、ネットワークから物理的に切り離した状態で保管しましょう。
- バックアップしたデータから、速やかに復旧できることを訓練等で確認しておきましょう。

サイバー犯罪の被害は警察へ通報を

- サイバー犯罪被害に遭ったかもしれないと思ったら、最寄りの警察署へ通報、ご相談ください。
- 警察ではお寄せいただいたサイバー犯罪に関する情報を分析し、事件捜査を行うほか、被害防止のための対策に必要な情報の提供・助言、他の企業への注意喚起等の取組を行っています。

警視庁では、サイバー犯罪やサイバーセキュリティに関する情報発信を行っています。

警視庁　サイバーセキュリティインフォメーション　検索

警視庁ホームページ

Twitter 公式アカウント

YouTube 警視庁公式チャンネル

我が社もサイバーセキュリティに万全を期すのじゃーっ!!

警視庁では、サイバー犯罪やサイバーセキュリティに関する情報発信を行っています。

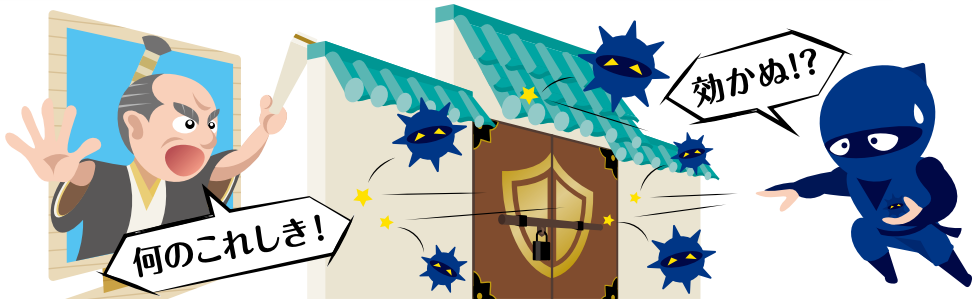
警視庁　サイバーセキュリティインフォメーション　検索

警視庁ホームページ

Twitter 公式アカウント

警視庁創立150年

対策1 脆弱性は速やかにパッチを適用する!!（修正プログラム）



- テレワークにも利用されるVPN機器の脆弱性から、組織内部のネットワークに侵入され、ランサムウェアに感染する場合があります。
- WEBサイトに脆弱性があると、攻撃者から勝手に内容を変更され、データの流出やWEBサイト閲覧者のウイルス感染につながることがあります（WEBサイト改ざん）。
- 脆弱性の解消は、メーカーから提供されるパッチ（修正プログラム）を適用する必要があります。常に脆弱性情報を収集し、速やかにアップデートしましょう。
- 脆弱性によりシステムの認証情報が漏れている場合があるので、パスワードの変更を検討しましょう。
- 使用しているシステムの保守を業者に委託している場合は、保守契約で脆弱性対応の有無を確認し、アップデート漏れがないようにしましょう。
- OS、ウイルス対策ソフト等は、必ず最新の状態にアップデートしましょう。

＜バージョン確認ツール／脆弱性の公表情報＞

MyJVN バージョンチェッカ	https://jvndb.jvn.jp/apis/myjvn
JVN iPedia（脆弱性対策情報データベース）	https://jvndb.jvn.jp/index.html

対策2 USBメモリ等の接続は厳格に管理する!!

- 許可のない機器を接続してはいけません。
- 許可のある機器でも、使う前にウィルスチェックをしましょう。
- 充電などでスマホを接続するとウィルスに感染することがあります。
  扇風機などのUSB機器も同様です。

対策3 メールの添付ファイルや本文のURLは安易に開かない!!

- メールに添付されたウイルス付きのファイルを開くことで、ウイルスに感染します。添付ファイルには、セキュリティ製品の検知を逃れるため、悪意のあるマクロを含んだOffice文書ファイルや圧縮ファイル、ショートカットファイルなど、様々なパターンがあります。
- メールやSMSの本文中に不正なURLリンクが書かれており、このリンクをクリックすると、外部WEBサイトに設置された不正なファイルをダウンロードさせられることもあります。
- 差出人名を、過去にメールを送受信した相手の名前に偽装し（なりすまし）、本文も、過去のメールを引用するなどして、正規のメールへの返信を装うメールを送信し、さらに感染拡大を図る攻撃（Emotet）が流行しています。
- 普段からやりとりをしている相手からのメールに見えても、添付ファイルや本文のURLは安易に開かないようにしましょう。

対策4 パスワードは複雑な文字列にする!!

- パスワードは、使い回さず、長く複雑なものに設定しましょう。
- IoT機器（ウェブカメラ・ルータ等）のパスワードは、乗っ取り防止のため、初期設定から変更しましょう。
- 各種ログイン機能の設定にアカウントロックアウト、接続IPの制限、多要素認証を活用しましょう。