

もし、ウイルス感染を確認したら

- ① まずは、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する。
- ② 社内のセキュリティ担当者へすぐに報告し、会社(組織)全体で現況を認識する。
- ③ 他のパソコンの感染実態も確認し、隔離した上、セキュリティ担当者またはセキュリティベンダーの指示を受けて対応する。

く知っておくだけでも是非!!>

少し前に流行ったランサムウェアに感染した場合、もしかしたら、「No More Ransom」というサイト内に用意されたツールの活用で、暗号化を解除できるかもしれません。

もしもの時のために、是非覚えておきたい一つです。

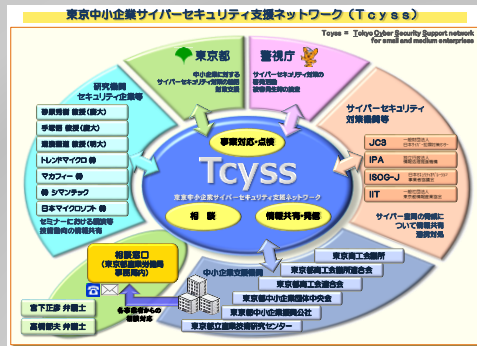
<https://www.nomoreransom.org/ja/index.html>

一人で悩まず
ご利用ください

困ったときには、相談を!!

サイバー犯罪の被害に遭ってしまったら、お近くの警察署までご連絡ください。

もし、警察へ相談していいものか悩んだときは、「東京中小企業サイバーセキュリティ支援ネットワーク(Tcyss)」の相談窓口を活用ください。



Tcyssは、東京都を中心に、警視庁、中小企業支援機関等と連携し、都内の中小企業を対象にサイバーセキュリティの支援を行うために設置した組織です。

社内のサイバーセキュリティ対策の強化や情報流出事案に関する各種相談に対応します!!



TEL03-5320-4773
東京都産業労働局商工部 相談窓口
 受付時間: 平日9:00~12:00 / 13:00~17:00
 東京都新宿区西新宿2-8-1 都庁第一本庁舎20階北側

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。

情報セキュリティ広場 検索



Twitter
@MPD_cybersec



警視庁公式
チャンネル
YouTube



警視庁サイバーセキュリティ対策本部

どんな形でやってくる!?

ランサムウェア対策

※ ランサムウェアは、利用者のファイルやフォルダを勝手に暗号化し、データへのアクセスを妨げた上で、暗号化の解除を条件に金銭(身代金)を要求してくる脅迫を伴った攻撃です。



USBメモリ

会社で使用許可を得ていないUSBメモリ等の接続



脆弱なシステム
公開されている脆弱性の修正プログラムの未適用



サイト改ざん

ブックマークしたURL以外への接続や、SMS・メール本文に付いているURLの軽率なクリック



メール

普段と文面等の印象が違う取引先からのメールの添付ファイルの開封



犯罪手口を把握していないと危険です!!



発見された脆弱性に対するパッチ (修正プログラム)の早期適用を

2021年に公表された脆弱性(システム上の穴)は**5,671件**(1日単純平均**15.5件**)。

この脆弱性の存在は、サイバー犯罪者も認識しており、その脆弱性が補正されていない対象を探し、悪用して金に換えてやろうと常に狙っています。

この穴をふさぐ方法として、そのシステム等を製作したベンダーから修正プログラムが公開されます。

修正プログラムが公開されたら、できるだけ早く修正プログラムを適用(インストール)して、犯罪者の侵入口となる穴を塞ぐようにしましょう。



<参考>脆弱性公表件数

年	年間公表数	単純平均
2016	8,939件	24件/日
2017	14,308件	39件/日
2018	15,707件	43件/日
2019	15,331件	42件/日
2020	15,807件	43件/日
2021	5,671件	16件/日

引用: JVN iPediaを元に集計

脆弱性の公表情報については

MyJVN バージョンチェック

<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>

で対象製品別に調べることができますので、定期的に確認し、安全な状態を保てるようにしましょう。

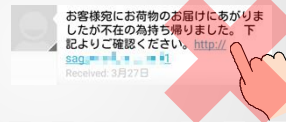
SMSのURLも要注意

フィッシング詐欺の犯行手口として有名になっているSMS(ショートメール)での犯行ですが、ランサムウェアを仕込んだサイバー犯罪としても悪用されています。

犯罪者からすれば、**どんな手段であっても、組織内へ侵入ができれば目的は達せられる**からです。

よく利用しているサイトから自社・自分宛に本文にURL付きのSMSが送られてきた場合は、本文中のURLはクリックせずに、その送信元となるサイトのホームページから入り直して(ブックマークしているような相手であれば、そのブックマークを利用して)確認するようにしましょう。

また、URLをクリックしてサイトに接続しただけでマルウェアに感染する可能性もあることを認識し、安易にクリックするのはやめましょう。



USBメモリ等の管理も厳格に

間く機会が少なくなったUSBメモリなど外部記録媒体による感染ですが、こちらも無視はできません。

会社での使用を認めていないUSBメモリなどの外部記録媒体を、会社に勝手に持ち込んで、会社のパソコンに挿してデータのやり取りをしていませんか。

また、**個人のスマートフォンを会社のパソコンにつないで充電**したり、ネットワーク内へ勝手に接続して、資料や個人情報のやり取りをしたりしていませんか。

さらに、それを見ても見ない振りしていませんか。

会社で把握できていない外部との接続が、今、感染原因の一つと言われ始めています。人・物の管理について見直してみましょう。



メールに添付されたファイルや本文のURLのクリックは慎重に

最近のサイバー犯罪で使われるメールには、犯罪者が取引先などの名義を使い、**差出人になりすましてメールを送る手口**が確認されています。

「.exe」と「.js」のアルファベットの記号(正式には「拡張子」と呼ばれるものです)が付いたファイルがメールで送られてきたときは、**直接マルウェアが送られてきたもの**と考えて、クリックしないようにしましょう。

その他、添付ファイルにマルウェアが仕込んであることをわからないようにするために、**アルファベット3文字の拡張子がついているoffice文書**(「.xls」「.doc」など)で、標準機能の**マクロ**という機能を悪用してきたり、ウイルス対策ソフトなどのセキュリティをすり抜けることを目的として、**パスワード付きの「.zip」ファイル**で送られてきたりします。

普段から使っているメールだからこそ、用心に用心を重ねて被害に遭わないようにしましょう。



.exe



.js



.xls



.doc



.zip

もしものためのバックアップ

既に災害対策用にクラウドサービスを利用してバックアップデータを保存している会社もあると思いますが、ランサムウェアによるサイバー犯罪では、**ネットワークに繋がったままの機器に保存されたデータは暗号化**されてしまうため、バックアップデータも使えなくされてしまう可能性があります。

バックアップデータは、ネットワークから外して保存するという手間がかかりますが、感染後の**早期復旧**のため、**事業継続**のために対策を取りましょう。

また、犯罪者が、被害者に金を払わせる確度をあげる手段として、機密情報等を盗み、公開と引き換えに金銭を要求する手口になっています。

重要データ等の保存は、盗られても中身を見られないようにするために、**暗号化して保存**することも一考してみてください。

