BASIC
Confertas Office

身を守るには
知ることから！

社内回覧用

情報セキュリティ被害の最新事例
2023年3月版

【大切なお願い】
会社を守るため、社長様、幹部様、従業員様、
パソコンやスマホを利用する**皆さまに回覧ください。**
自分事で実態を知ることが対策の第一歩です。

【この冊子の活用の仕方】
この冊子では、セキュリティの最新情報を月刊で
お伝えしています。被害事例を**自社に置き換えて、**
対策と意識向上にお役立てください。

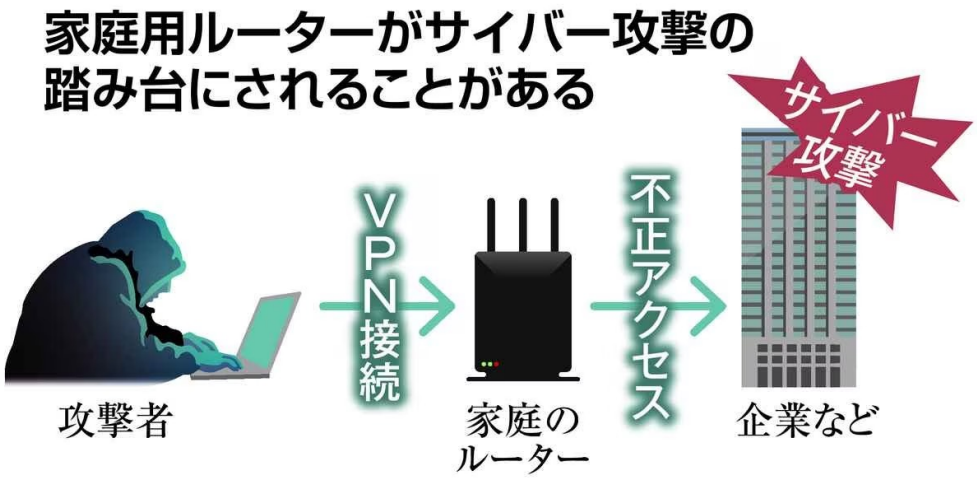
BASIC
Confertas Office

■家庭用ルーターサイバー攻撃の踏み台に　警視庁確認

2023年3月28日

・警視庁公安部は２８日、家庭用のインターネットルーターが複数の企業のサイバー攻撃に「踏み台」として悪用されていたことを確認したと明らかにした。こうした悪用は令和２年ごろから増加し、従来の対策のみでは対応できないことも判明したという。

・公安部のサイバー攻撃対策センターによると、民間の複数の大手企業がサイバー攻撃された事案を詳しく分析するなどした結果、攻撃者が、ＶＰＮ（仮想私設網）を介して一般家庭のルーターに侵入。そこから企業にサイバー攻撃を仕掛けていたことが分かったという。サイバー攻撃対策センターは「ルーターの持ち主が攻撃を仕掛けたように見せかけた」とみている。



・一度侵入を許すと、ルーターのソフトを最新のものにするといった従来の対策などを行っても、攻撃者は侵入を続けられることも確認。サイバー攻撃対策センターは「気付かないうちに永続的に踏み台にされている人も多い」とする。

・確認の際、身に覚えのないＶＰＮ設定や知らないユーザーが追加されている場合は、踏み台にされている可能性が高く、初期化などを推奨するという。サイバー攻撃対策センターの蓮沼正英副所長は「踏み台にされると思わぬトラブルに巻き込まれる可能性がある」として注意を促した。

リモートワークも増えきました。多岐に渡る脅威に対して、適切な対策を取ることが引き続き求められますね。
専門家に相談し、対策を施しましょう。

■画像：下記出典記事より
■出典：産経新聞
https://www.sankei.com/article/20230328-75WZ6GGGANODZI5KZT3WLYSITU/

BASIC Confertas Office

■東京電力や東京ガスをかたるフィッシング詐欺に注意！料金請求メール装う手口。

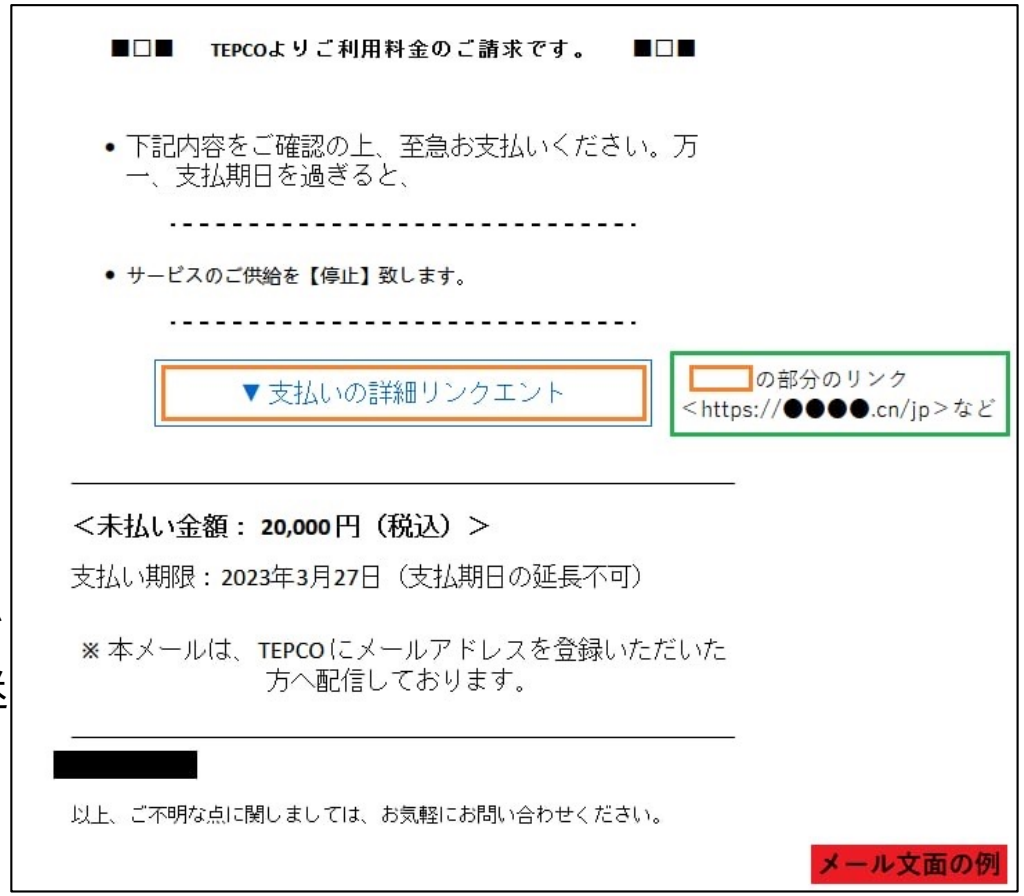
2023年3月28日

・フィッシング対策協議会は3月28日、東京電力や東京ガスをかたるフィッシングの報告が増えていると注意喚起した。28日時点で当該フィッシングサイトは稼働中。

・「東京電力エナジーパートナー」や「myTOKYOGAS」をかたって利用料金請求メールを送り、メール本文のリンクからフィッシングサイトに誘導、個人情報を入力させる手口。

・フィッシング対策協議会は一般ユーザーに対し、このようなフィッシングサイトでログインIDやパスワード、Vプリカ発行コード番号、額面などを入力しないように呼び掛けている。

・フィッシングサイトは本物のサイト画面をコピーして作成することが多く、見分けるのは非常に難しい。対策としてメールサービスの迷惑メールフィルターを活用すること、ログイン時にはメールなどのリンクではなく、公式アプリやブラウザのブックマークなどからアクセスすることを推奨している。



他にも、AmazonPrimeや佐川急便、PayPay銀行などをかたるフィッシングメールについての報告が見られました。引き続き注意が必要ですね。

■画像：下記出典記事より、実際のメール文面の例
■出典：Yahoo!ニュース ITmedia NEWS
https://news.yahoo.co.jp/articles/139ea6f8f447e3cb25dc795799efb7ceb074b21a

BASIC Confertas Office

■マルウェア「Emotet」に新しい感染手口。IPAが「OneNote」経由の攻撃を注意喚起

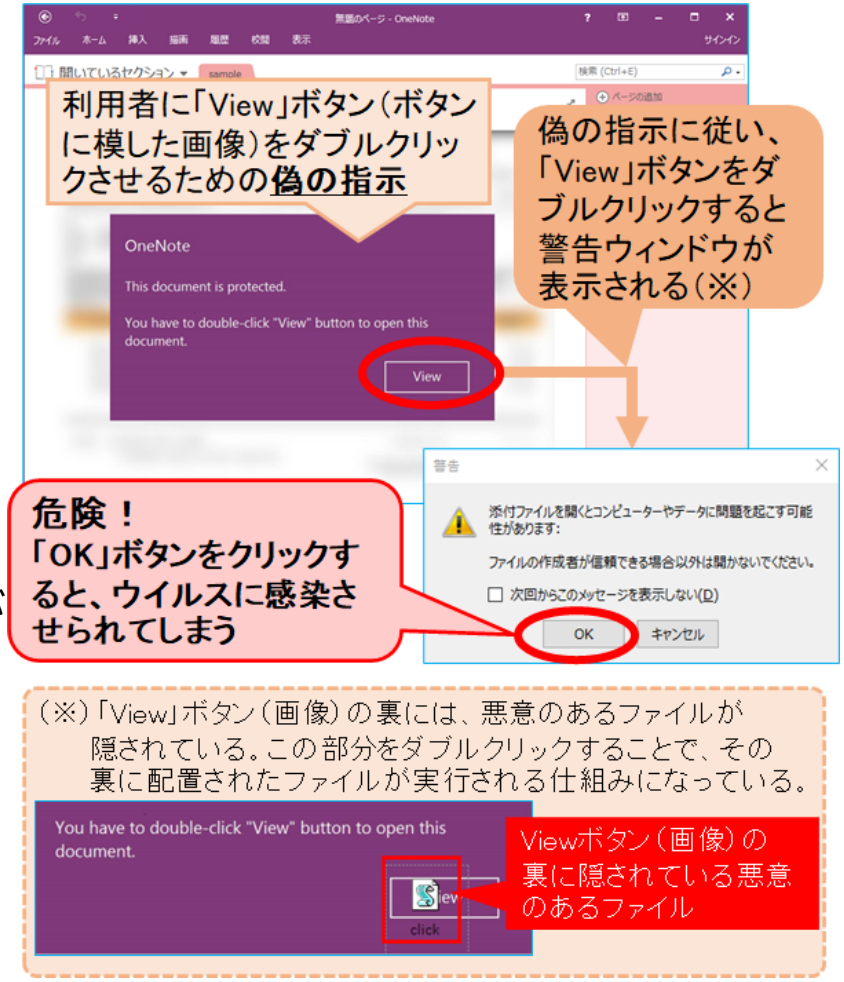
2023年3月20日

・独立行政法人情報処理推進機構（IPA）は3月17日、マルウェア「Emotet」の新たな感染手法を確認したと発表した。今度は「Microsoft OneNote」形式のファイル（.one）がターゲットになっているという。

・「Microsoft Office」がなくても感染する亜種も確認されている。昨年末に終息したかに思われたが、今月に入ってまた活発化しつつあるとのことで警戒が必要だ。

・IPAによると、今回新たに確認された手法は「Microsoft OneNote」形式のファイルになっており、ファイル内に書かれた偽の指示に従ってボタンに模した画像をダブルクリックすると、その裏に隠されている悪意あるファイルが実行され、「Emotet」に感染する仕組みとなっている。

・IPAは、メールのリンクや添付ファイルを不用意に開かない、OSやアプリケーション、セキュリティソフトを常に最新の状態にする、編集やマクロのブロックを安易に解除したり、警告ウィンドウを無視したりしないといった、基本的な対策を怠らないよう呼び掛けている。



■画像：IPAのWebサイトから引用
■出典：窓の杜
https://forest.watch.impress.co.jp/docs/news/1486966.html

Emotetは、「Excel」や「Word」経由で感染すると思い込んでいると、騙されてしまう可能性があるので注意しましょう。

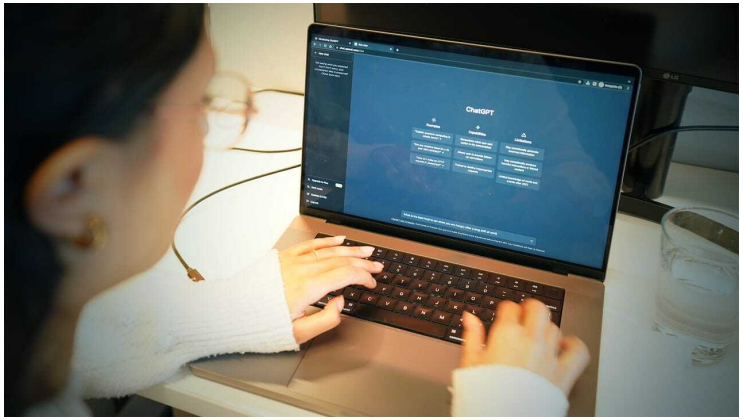
■「ChatGPT」の名称を悪用したマルウェアが出現。「Chrome」拡張機能を装う

2023年3月14日

・「ChatGPT」は、基本的にユーザーのどのような質問にも会話形式で答えられるとあって、今最もホットな話題の1つ。それだけに、詐欺師が自分の利益のために悪用しようとするのは、時間の問題だったようで、すでにそうした事例が発生。

・ChatGPTをかたる「Chrome」拡張機能が「Chromeウェブストア」に公開され、インストールしたユーザーが被害に遭ったという。この拡張機能「Quick access to Chat GPT」は、名前のとおり、ChatGPTへの連携機能を提供するという触れ込み。ところがこれは「Facebook」アカウントを乗っ取る機能も備えていた。

・Facebook上で宣伝されていたこの拡張機能は、ユーザーがクリックしてインストールすると、クッキーやFacebookアカウントのデータを収集する。アカウントを乗っ取ると、このマルウェアの宣伝にアカウントを利用してネットワークの拡大を図っていたという。



■画像：ChatGPT（June Wan/ZDNET）

この種のなりすまし詐欺の拡張機能は珍しくないため、Chrome拡張機能をインストールする際には注意が必要ですね

■出典：CNET JAPAN
https://japan.cnet.com/article/35201232/

■ウイルス対策ソフトを無効にしてデータを盗み、ランサムウェアを仕掛けるマルウェア「Royal」の脅威

2023年3月8日

・Royalは2022年9月頃から確認されており、アンチウイルスソフトを無効にして大量のデータを流出させた後、最終的にランサムウェアを展開してシステムを暗号化するマルウェアとされている。

・このランサムウェアの初期アクセスは一般的にフィッシングメールとされている。その他にもリモートデスクトッププロトコル(RDP: Remote Desktop Protocol)の侵害や公開アプリケーションの悪用、初期アクセスブローカ(IAB: Initial Access Brokers)経由によるシステムへの侵入が多いことも判明している。

・米国土安全保障省サイバーセキュリティ・インフラストラクチャセキュリティ庁はRoyalの被害者にならぬよう、既知の悪用された脆弱性を優先して修復することやフィッシングに関するユーザー教育を行うこと、多要素認証(MFA: Multi-Factor Authentication)を有効化するなどのセキュリティ対策を実施するよう推奨している。また、身代金を支払ったとしても暗号化されたファイルが復元される保証はないとし、たとえランサムウェアに侵害され身代金を要求されたとしても絶対に支払わないよう注意を呼びかけている。

ウイルス対策ソフトだけに頼るのは、危険な時代となりました。一度セキュリティの専門家へ相談してみましょう。

■出典：TECH+　マイナビニュース
https://news.mynavi.jp/techplus/article/20230308-2608578/

BASIC
Confertas Office

■TikTokは中国の「トロイの木馬」－米国家安全保障局サイバー責任者

2023年3月28日

・米国家安全保障局（ＮＳＡ）のサイバーセキュリティー部門責任者ロブ・ジョイス氏は27日、人気の中国系動画投稿アプリ「ＴｉｋＴｏｋ（ティックトック）」は中国の「トロイの木馬」であり、長期かつ戦略的なサイバーセキュリティー上の懸念をもたらしていると指摘した。

・ジョイス氏はカリフォルニア州ナパで開催された会議で、「なぜ要塞（ようさい）にトロイの木馬を引き入れるのか」と問いかけ、「中国側は米市民に見せたいものを加え、米市民に知られたくない自国に不利なものを削除するというデータの操作ができる。なぜそうした能力を米国に持ち込むのか」と語った。

・政治家やサイバーセキュリティーの専門家は、ＴｉｋＴｏｋの親会社である中国の字節跳動（バイトダンス）が月間１億5000万人の米ユーザーを把握し過ぎているとの懸念を繰り返し示しており、ＴｉｋＴｏｋ側がデータ分離のため講じた措置では、情報入手を試みる中国政府の関与を防ぐには不十分だと主張している。

TikTokは若者世代を中心に日本でも流行しており、例外ではありません。公用端末での使用を禁止したり、国民の使用に関して制限を設けようとする国も出てきました。直接業務と関係のないアプリケーションでもどこから情報漏洩があるかわからないので注意が必要ですね。

■出典：Yahoo!ニュース　Bloomberg
https://www.data-max.co.jp/article/61257

情報セキュリティ対策は、実績豊富で信頼できる企業をお選びください。

最近は、ランサムウェアや情報漏えいなど、経営に関わるサイバー攻撃の被害も増加し、ひとつの社会問題となっています。私たちは、「サイバー攻撃の脅威からお客様を守りたい」そして、「今後もお客様と一緒に永く成長していきたい」と強く思っています。

情報セキュリティは、社内ネットワークに関わる重要な部分であり、信頼できる会社と付き合うことが大切です。私たちは、お客様に正確な情報と知識、安心の技術サポートを提供できる体制を整えていますので、ぜひご安心ください。