事業者向け
サイバーセキュリティ対策

～サイバー攻撃で事業活動を止めないために～

【体験型サイバーセキュリティセミナー版v18.60】

滋賀県警察　サイバー犯罪対策課

本日の内容

1. サイバー空間の脅威の情勢（一般向け）
   - 体験：サポート詐欺
2. 企業を取り巻くサイバー空間の脅威の情勢
   - 体験：ランサムウェア
   - 体験：標的型メール攻撃
3. サイバーセキュリティ対策のポイント

【今日のポイント】

サイバーセキュリティ対策は、サイバー攻撃の手口を知ることが重要です。

- **サイバー攻撃の体験を通して手口と対策を知ってください。**
- **一人ひとりができる対策を行うことで被害を防止することができます。**
- **経営者や管理者が行うべき基本的なサイバーセキュリティ対策を知ってください。**

1　サイバー空間の脅威の情勢

- **最初に、サイバー空間の脅威の情勢や現在のインターネット情勢を説明します。**
偽ショッピングサイト詐欺、サポート詐欺の体験と対策について説明します。

令和５年上半期のサイバー空間の脅威の情勢（警察庁）

警察庁が公表した令和５年上半期における「サイバー空間をめぐる脅威の情勢」を紹介します。（令和5年９月21日公表）

サイバー空間 ➡ 社会経済活動を営む重要かつ公共性の高い場へと変貌
国内外で様々なサイバー事案が発生

サイバー攻撃の情勢

- 大手システム事業者、電子部品関連企業に対する不正アクセスや、特定の事業に対する標的型メール攻撃が確認された。
- DDoS攻撃とみられるWebサイトの閲覧障害が複数発生した。

インターネットバンキング不正送金

- 発生件数2,322件（前年比104.4%増加）
- 被害額約29億円（前年比97.2%増加）
- 被害の多くはフィッシングによるもので、金融機関を装ったフィッシングサイトへ誘導するメールが多数確認

R5年被害
約80億円

フィッシング等の被害

- フィッシング報告件数は、右肩上がりで増加。
  前年同期比17.9%増加（フィッシング対策協議会）
- クレジットカード不正利用被害額121.4億円。
  前年同期比21.3%増加（日本クレジットカード協会）

ランサムウェア被害

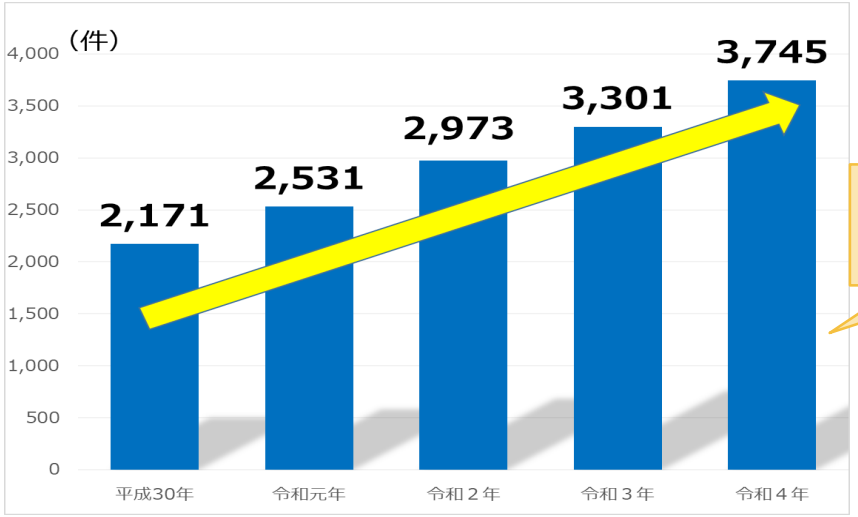
- 被害件数103件（前年同期比9.6%減少）
- データの暗号だけでなく、データを窃取した上、事業者に対して「対価を払わなければ当該データを公開する」等と対価を要求する二重恐喝が多くを占める。

サイバー空間における脅威は極めて深刻な情勢が続いています。

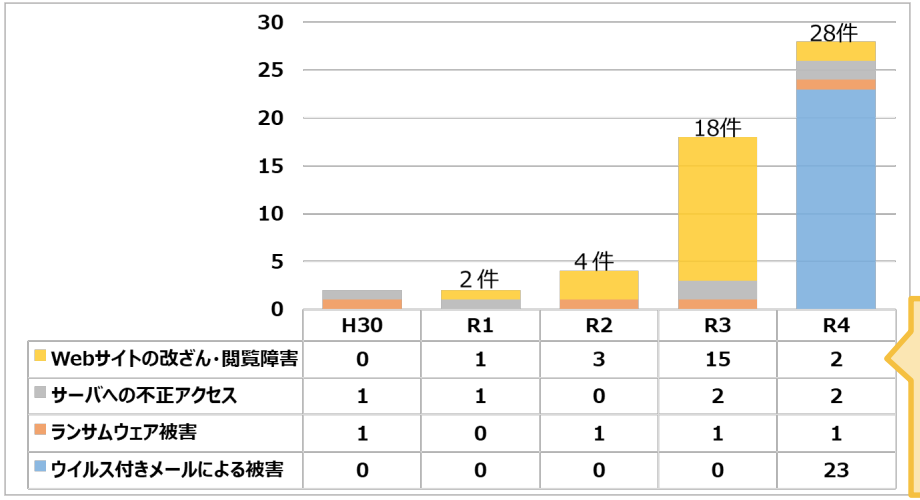
引用：警察庁｜統計「令和５年上半期におけるサイバー空間をめぐる脅威の情勢等について」
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R05_kami_cyber_jousei.pdf

令和４年：サイバー空間の脅威の情勢（滋賀県）

滋賀県の令和４年の「サイバー空間をめぐる脅威の情勢」を紹介します。



R5.8月現在
2,161件



	H30	R1	R2	R3	R4
Webサイトの改ざん・閲覧障害	0	1	3	15	2
サーバへの不正アクセス	1	1	0	2	2
ランサムウェア被害	1	0	1	1	1
ウイルス付きメールによる被害	0	0	0	0	23

R5.4に県議会、大津市議会、草津市議会のＨＰが閲覧障害

サイバー犯罪関連相談件数

- 令和４年3,745件（前年＋444件）
- **過去5年間、顕著な増加傾向**
- クレジットカード番号窃取に関する相談は、前年の**約11.5倍と急増**
- 主な相談
  - **フィッシング（ID・パスワードの窃取）**
  - **偽ショッピングサイトの詐欺**
  - **サポート詐欺、ロマンス詐欺、投資詐欺**

事業者へのサイバー攻撃に係る事案の認知件数

- 令和4年28件（前年＋14件）
- 事業者へのサイバー攻撃は増加傾向
- 規模や業種を問わず被害が発生
- 令和４年は特にEmotetと呼ばれるウイルス付きメールの受信が増加
- 被害が潜在化している可能性がある。

特に相談が多い4つの事例

サイバー犯罪に関する相談の多くは、以下の４つです。

滋賀県警察 サイバーセキュリティ情報SHIG@
サイバー犯罪からあなたを守るセキュリティ情報をお届けします。

フィッシング

フィッシングは、メールやSMSを使ってユーザーを偽サイトに誘導し、**ID・パスワード**や**クレジットカード情報**等を入力させて、それらの情報を盗み取る手口です。

ID・パスワードを盗み取られたら・・・
- ショッピングサイトで**無断で買い物**をされる。
- クレジットカードを無断で使用される。
- **闇サイト**で個人情報を売られる。
- パスワードを変更される。

【被害防止】
- メール等に記載されたリンク（URL）をクリックしない。
- ID・パスワードは、必ず**公式サイト**から入力。

偽ショッピングサイト詐欺

偽ショッピングサイトは、**本物のサイトをコピー**したり、実在する会社名や代表者名を使用するため、見分けることが難しくなっています。会社が存在するか、連絡先が正しいかを確認してください。

特に**要注意なドメイン**
「**.top**」「**.xyz**」
「**.site**」「**.online**」
これらのドメインがついたURLは**偽サイト**の可能性が高いです。

STOP!
振込

【偽サイト見分けるポイント】
- **商品の支払い方法が銀行振込だけでないか。**
  偽ショッピングサイトの多くは、銀行振込しか利用できません。（入金後すぐに出金が可能であるため）
  会社が経営しているのに個人名義であったり、外国人名義の口座も要注意です。

サポート詐欺

サポート詐欺は、画面に突然、**偽のセキュリティ警告**等のメッセージを表示させたり、偽のウイルス感染を音声で知らせたりするなどして、ユーザの**不安を煽り**、画面に表示された電話番号に電話をかけさせ、パソコンを遠隔操作するソフトウェアをインストールするように促し、有償のサービス契約や**サポート料金を請求**する手口です。

STOP!
電話

【被害防止】
- 警告は偽物です。**電話しないでください。**
- 偽警告画面は、「×」ボタン等で消すことができます。

投資や副業を装った詐欺

SNSや**マッチングアプリ**等を通じて、知り合った人から、**投資**や**副業**等の話を持ち掛けられて、金銭（暗号資産）を**だまし取られる**ケースが発生しています。

- ◆ SNSで異性と知り合って、投資を勧められた。
- ◆ 外国人から資金を送る協力を依頼された。
- ◆ 余命宣告を受けた人から遺産を譲りたいと言われた。
- ◆ 話を聞くだけで**稼げる**と言われた。
- ◆「〇〇を評価するだけの仕事」を紹介された。

【ロマンス詐欺】
外国人などを名乗り、ネットで知り合った相手に恋愛感情を抱かせて現金をだましとる手口。

STOP!
送金

【被害防止】
- **「儲かる話」**は信用しないでください。
- 投資や金銭（暗号資産）の送金は**慎重**に行ってください。

体験コンテンツしていただけます。

サポート詐欺の概要

サポート詐欺とは

インターネット利用中、画面にウイルス感染を装ったメッセージを表示させ、サポート名目で費用を請求する行為

片言の日本語
電話をかけると、多くの場合日本語を話す外国人が対応する。

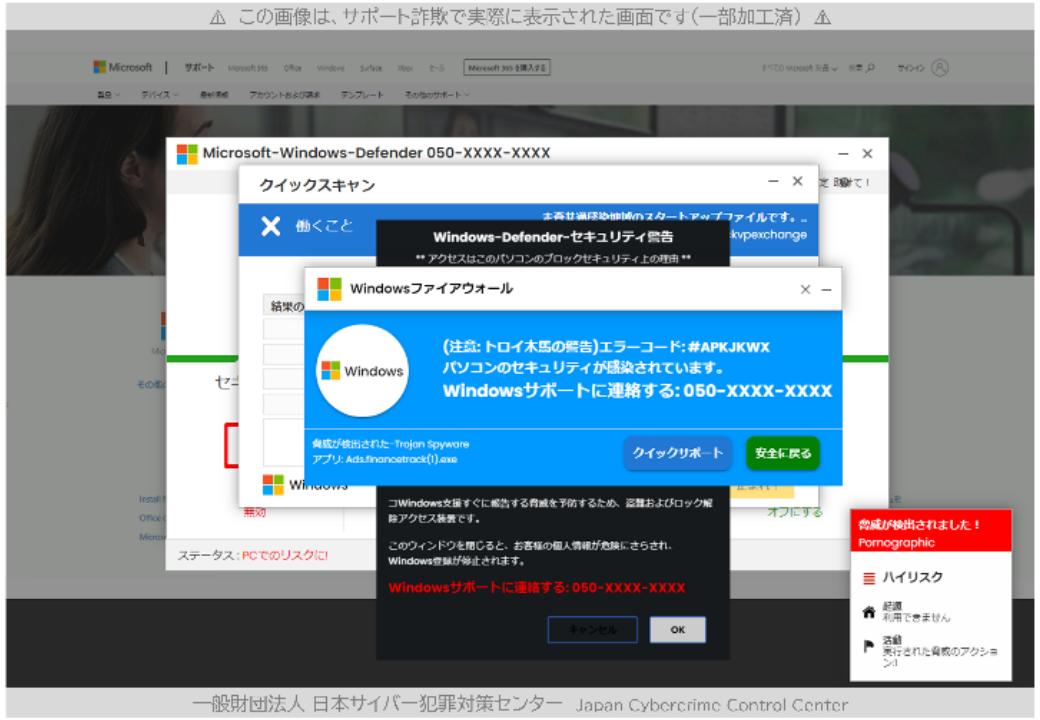
マイクロソフトの「ジョン」です。
ウイルス感染していますねェ

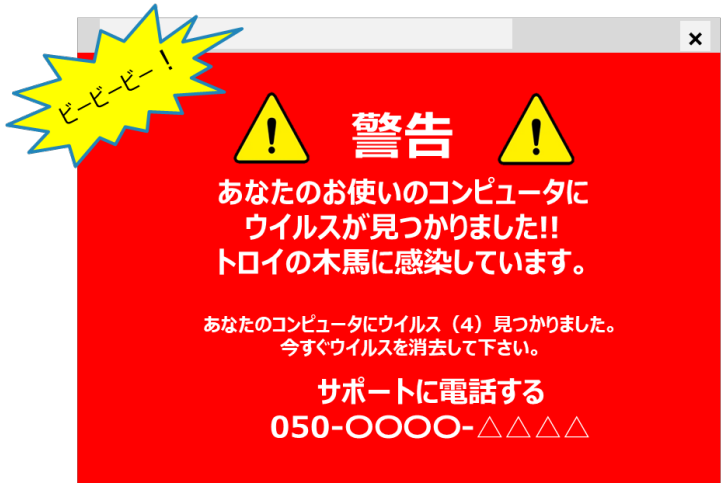
遠隔操作
遠隔操作ソフトをインストールさせられる。

遠隔でサポートします。
ソフトをダウンロードしてくださいネ。

ギフトカード
費用はGooglePlayカード等で支払わせる。

サポート料金は3万円です。保障プランは3年、5年があります。ギフトカードで払って下さい。おっと、電話は切らないでコンビニに行ってください。





サポート詐欺の仕組み

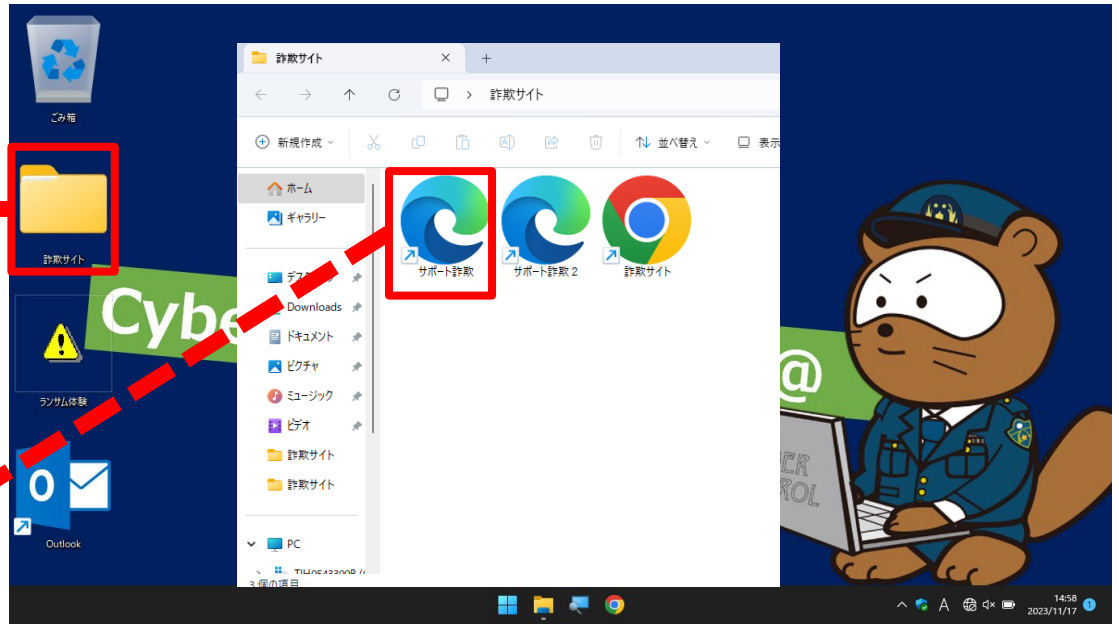
サポート詐欺の画面を体験しましょう。

1. デスクトップにある「詐欺サイト」フォルダを開いてください。

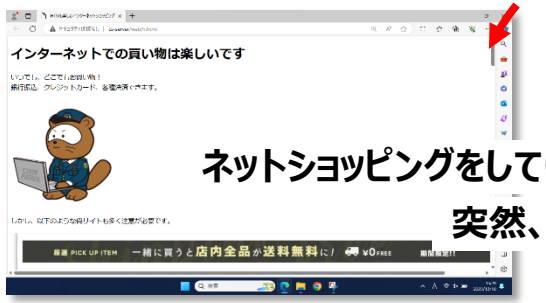
2. 「サポート詐欺」を開いてください。

※音が出ますので注意してください。

ダブルクリック



ダブルクリック

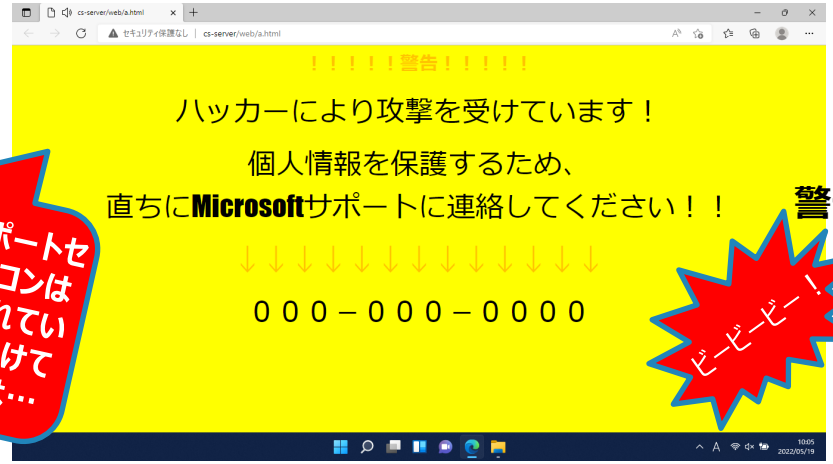


ネットショッピングをしていると・・・

突然、画面が変わり・・・

音声

こちらはマイクロソフトサポートセンターです。あなたのパソコンはマルウェアの脅威にさらされています。ただちにサポートを受けて下さい。個人情報の流出は…



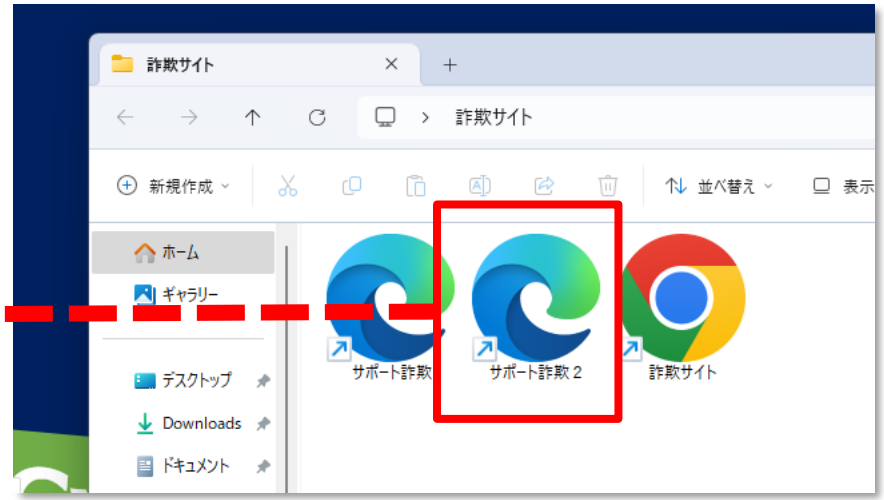
警告音

ビービービー！

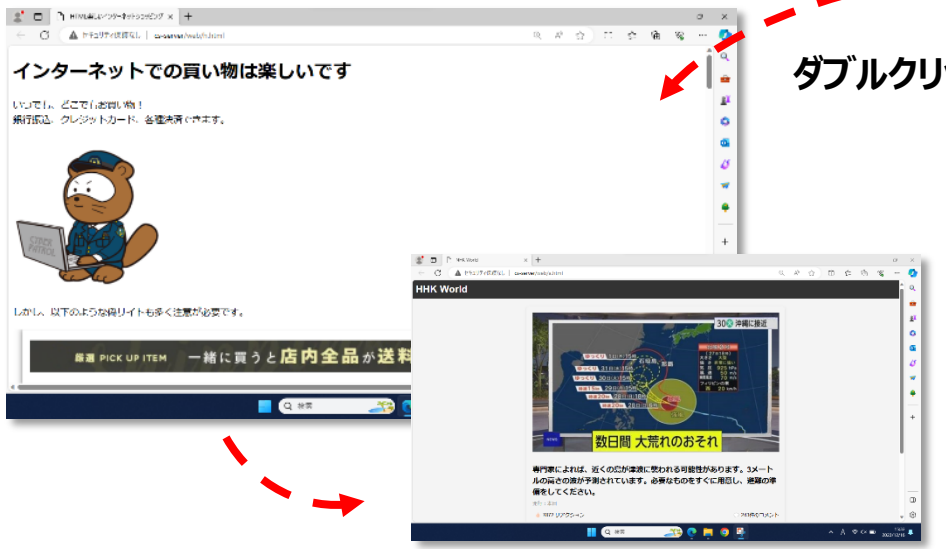
3. 「警告」画面が表示されますので、「×」ボタンで閉じて下さい。

サポート詐欺の仕組み

4．×ボタンがないパターンもあります。
デスクトップにある「詐欺サイト」フォルダの
「詐欺サイト２」を開いてください。

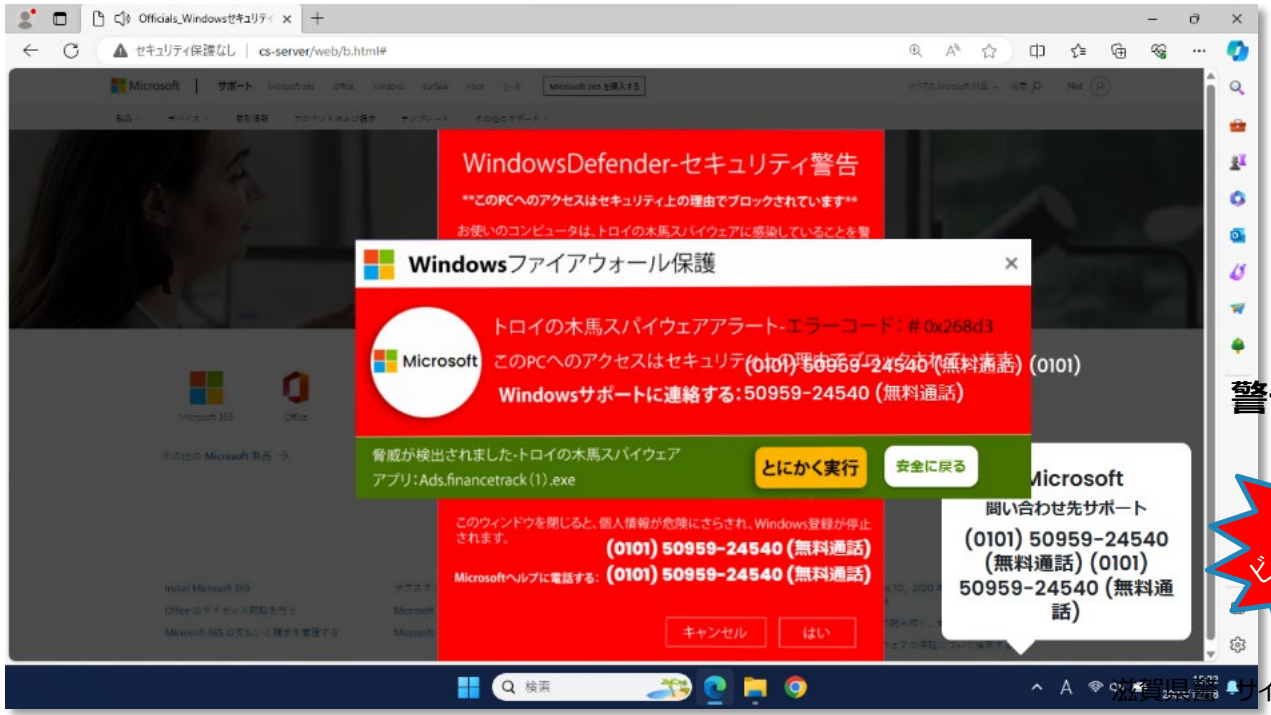


ダブルクリック



ネットショッピングをしていると・・・

突然、画面が変わり・・・



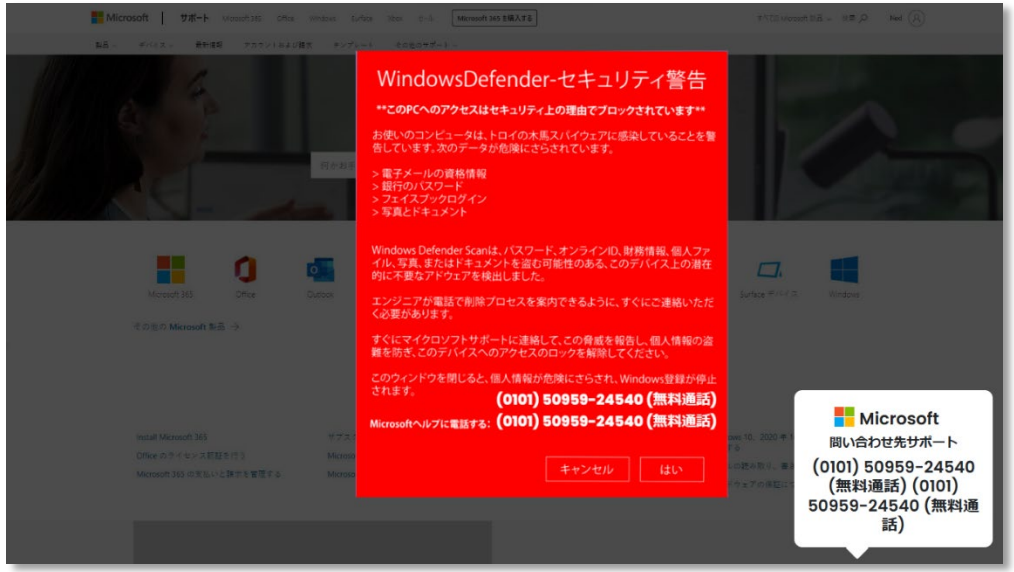
音声

警告音

ピーピーピー！

サポート詐欺（警告メッセージの消し方1）

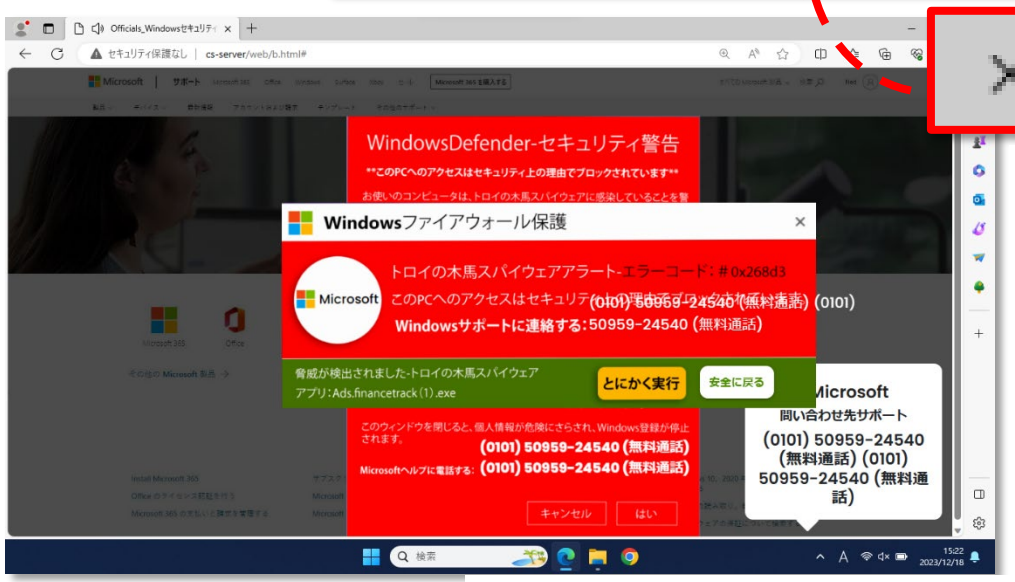
5. ×ボタンがない場合は、全画面表示になっている可能性があります。
ESCキーを押して、全画面を終了させると×ボタンが表示されます。
（ESCキーを長押しすると×ボタンが出る場合もあります。）



全画面表示になっていて、×ボタンがない。

ESCキー
（エスケープキー）
を押す。または長押し。

移動を押すと画面が消える

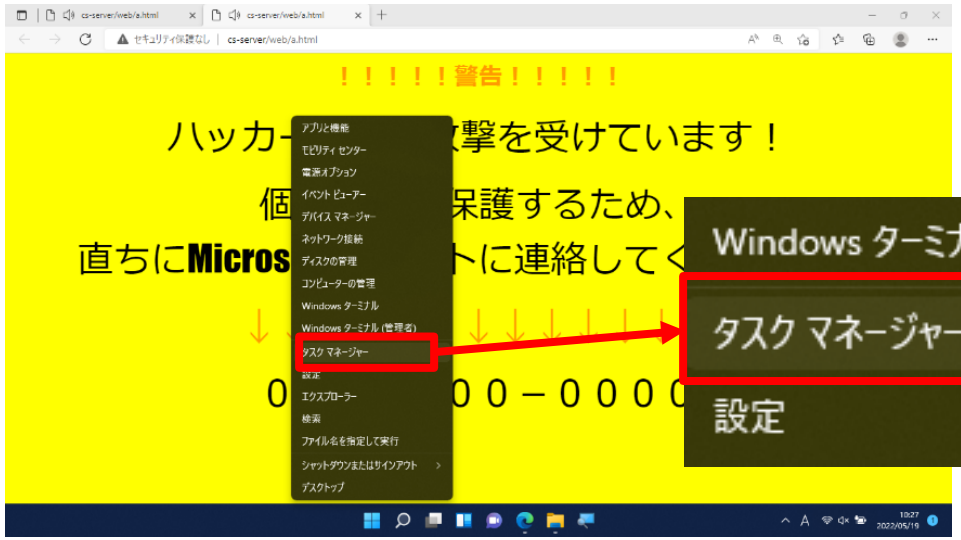


×ボタンが表示される

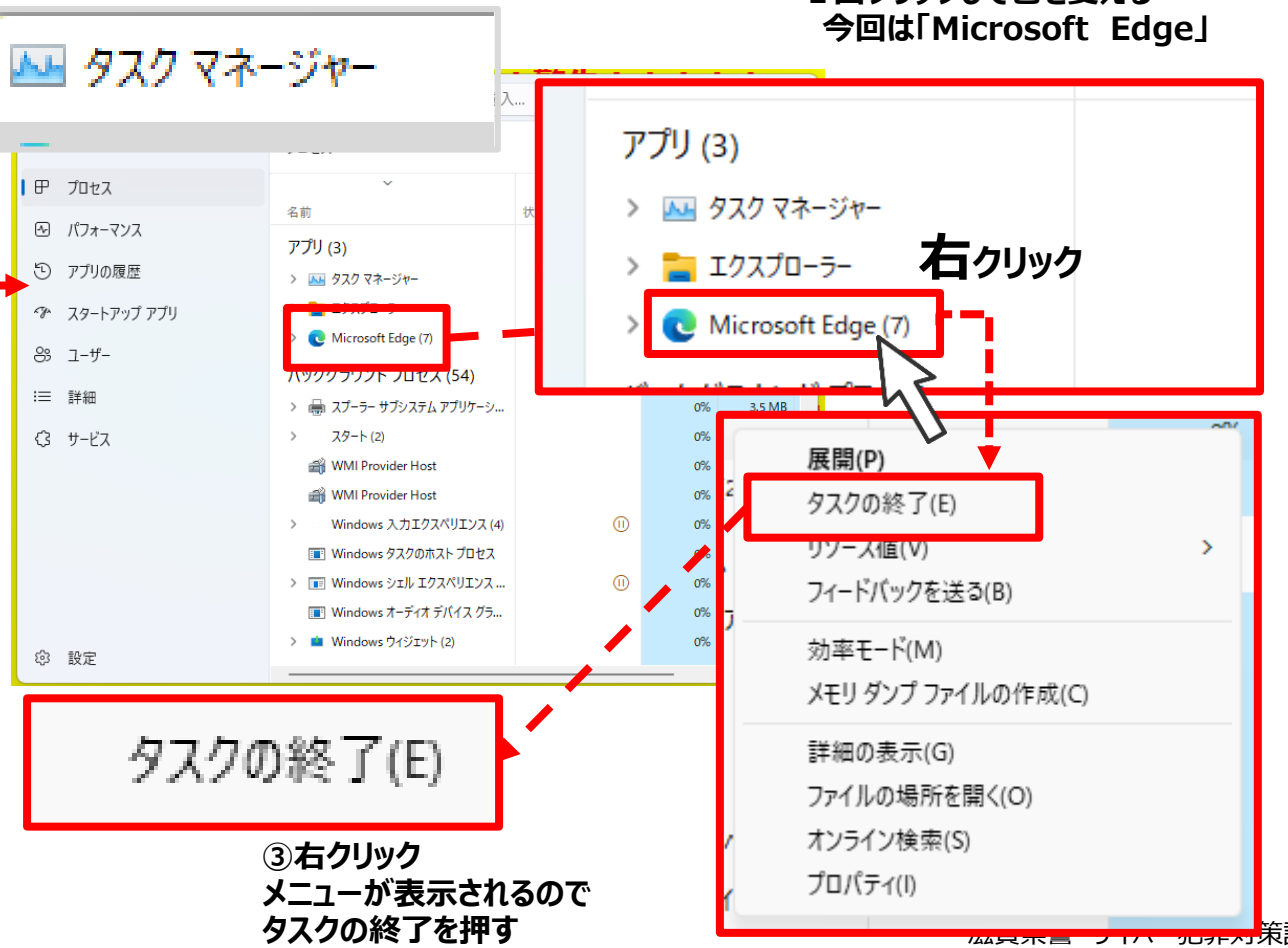
全画面表示が終了する。

サポート詐欺（警告メッセージの消し方2）

6．タスクマネージャーの中から「Microsoft　Edge」を選択して「タスクの終了」を押してください。

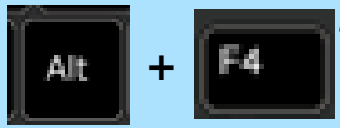


①Windowsアイコンを右クリック→タスクマネージャーを選択

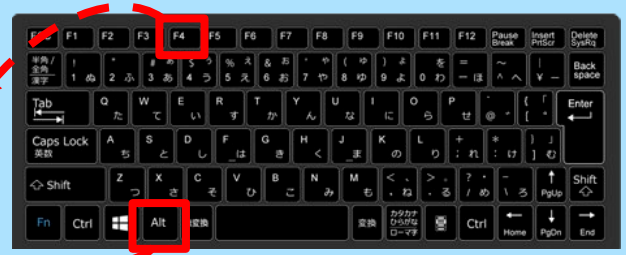


【裏技】画面一番上のアプリの強制終了

キーボードの「Alt」+「F4」を同時に押すと一番上のウインドウに表示されたアプリが終了できます。



Altキー　F4キー



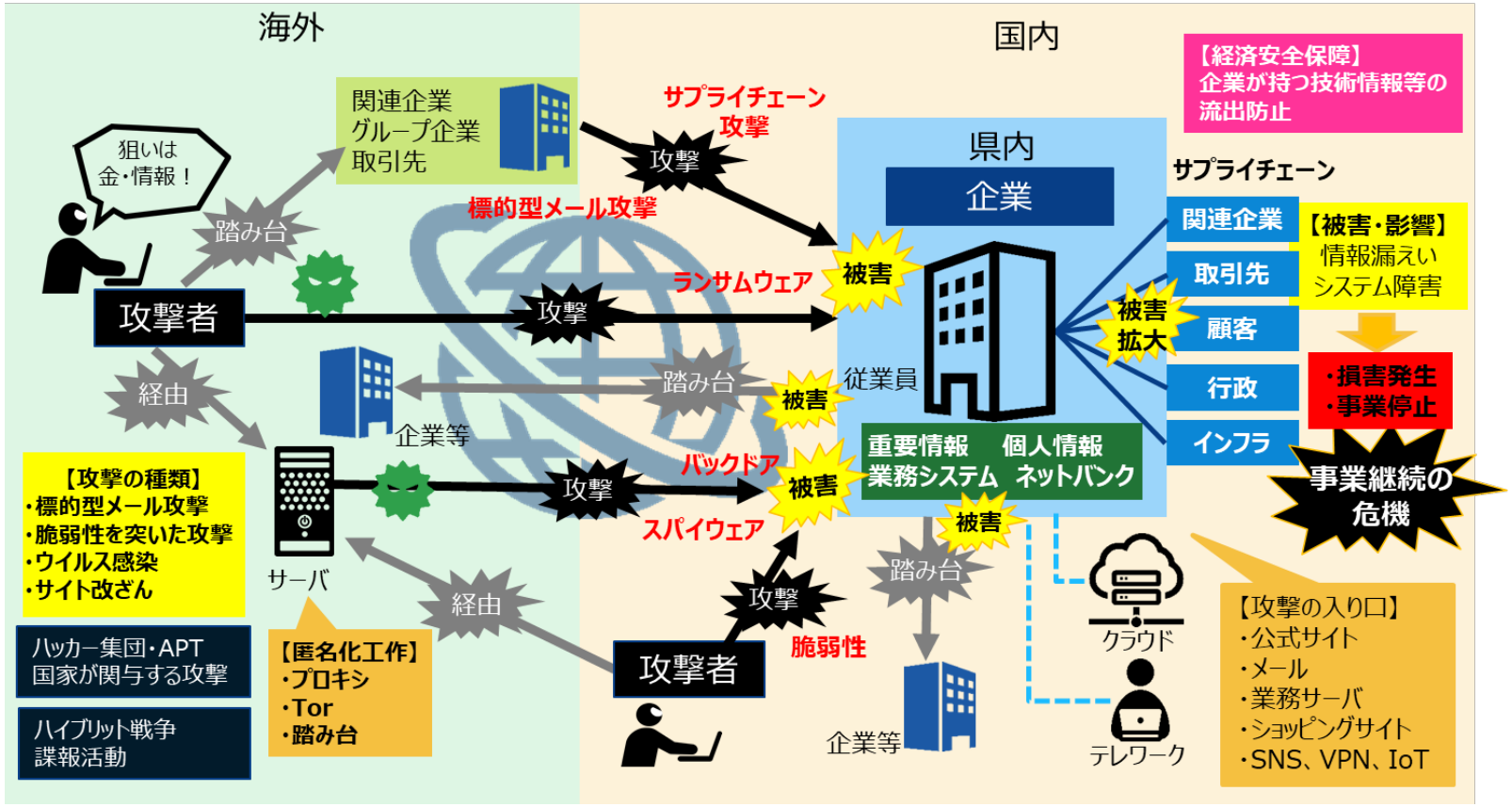
サポート詐欺の対策

【ポイント】

- 警告は偽物です。
  通常のWebページに表示されているか又はポップアップ機能を利用しています。
- マイクロソフトやウイルス対策ソフトが、電話をかけさせることはありません。
- 電話は絶対にしないでください。
- ギフトカードで支払いを求めるような行為は詐欺を疑って下さい。
  （遠隔操作でインターネットバンキングから送金させる手口もあります）
- 偽の警告画面は消すことができます。
  （画面が消えない場合は、電源を切ってください）
- 万が一、遠隔操作された場合は、端末を初期化することをお勧めします。

企業を取り巻くサイバー空間の情勢

サイバー攻撃は、複雑化・巧妙化しています。被害を受けると多方面に影響を及ぼします。



【事業活動の状況】

- 事業にはインターネットやパソコンが不可欠。
  - DX化
  - インボイス
  - 電子帳簿
- サプライチェーンで多くの企業と連携。
- 公式サイト、メール、サーバのほかテレワークやWeb会議が攻撃の入り口に。
- 攻撃を受けていることに気づかないことも。

攻撃 → 損害発生
情報流出
被害拡大
事業停止

事業継続の危機

ダメージは、個人の生活や経済界、社会に及ぶ。
経済安全保障にも影響。

【サイバー攻撃の特徴】

- 攻撃の目的は、金銭、情報。
- 企業の業種や規模は、関係なし。
- 海外から県内の企業に直接攻撃。
- サプライチェーンを使って間接攻撃。
- 海外サーバ経由で匿名化工作。
- 踏み台にされて攻撃に加担させられる。
- ランサムウェアの脅威が増加
- デマやフェイクニュースを使った情報戦も。

事業継続ができる体制を

- サイバー攻撃は完全に防ぐことが困難になっています。
- サプライチェーン上に被害が拡大するおそれがあります。

【対策のポイント】

攻撃を受けた場合でも被害を最小限にして、事業が継続できるように対策を考えておく必要があります。

防御
・アクセス権の強化
・暗号化
・分散管理
対処
・流出量の把握
・個人情報保護委員会への報告
・顧客への対応

サイバー攻撃の被害

情報漏えい　　システム障害

脆弱性への対応
・セキュリティパッチの適用
・アップデート
バックアップの取得
バックアップから復旧手順の確認

損害発生・事業停止

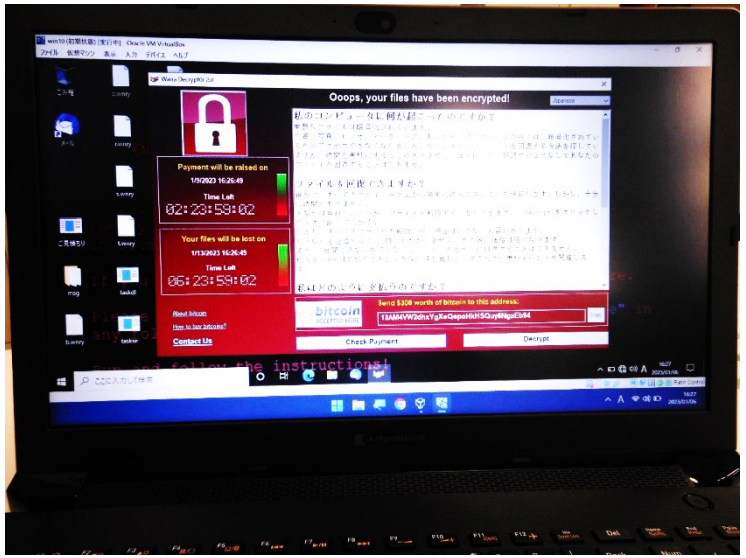
- リスクマネジメント（分析・評価・対策）・・・リスクファイナンシング
- インシデントレスポンス（被害発生時の対応要領）
- 災害として対応（BCPに基づく）

ランサムウェアとは

ランサムウェアとは、感染すると端末等に保存されているデータを暗号化して使用できない状態にした上で、そのデータを復号する対価として金銭を要求する不正プログラムです。

ランサムウェアは「ransom」（身代金）と「malware」（マルウェア⇒不正プログラム）を組み合わせた造語です。

このウイルスは、使用不能な状況を復旧することと引き換えに、金銭（暗号資産）を要求することから「身代金要求型ウイルス」とも呼ばれています。



ランサムウェア（WannaCry）に感染したパソコンの状況

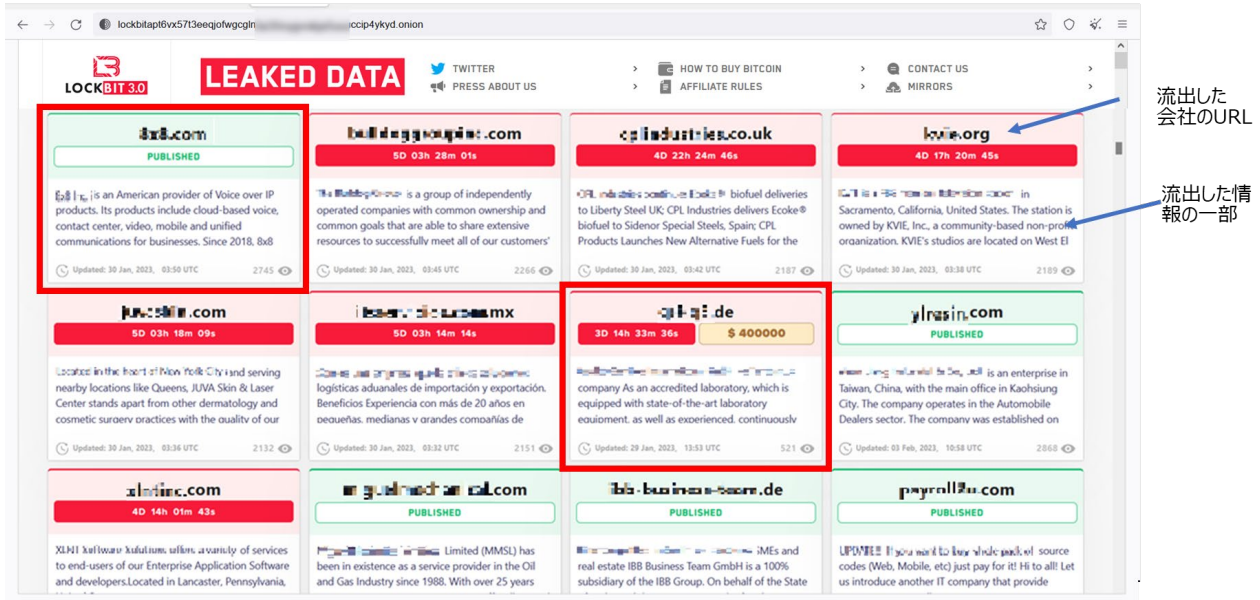
ランサムウェア（LOCKBIT2.0）に感染したパソコンの状況

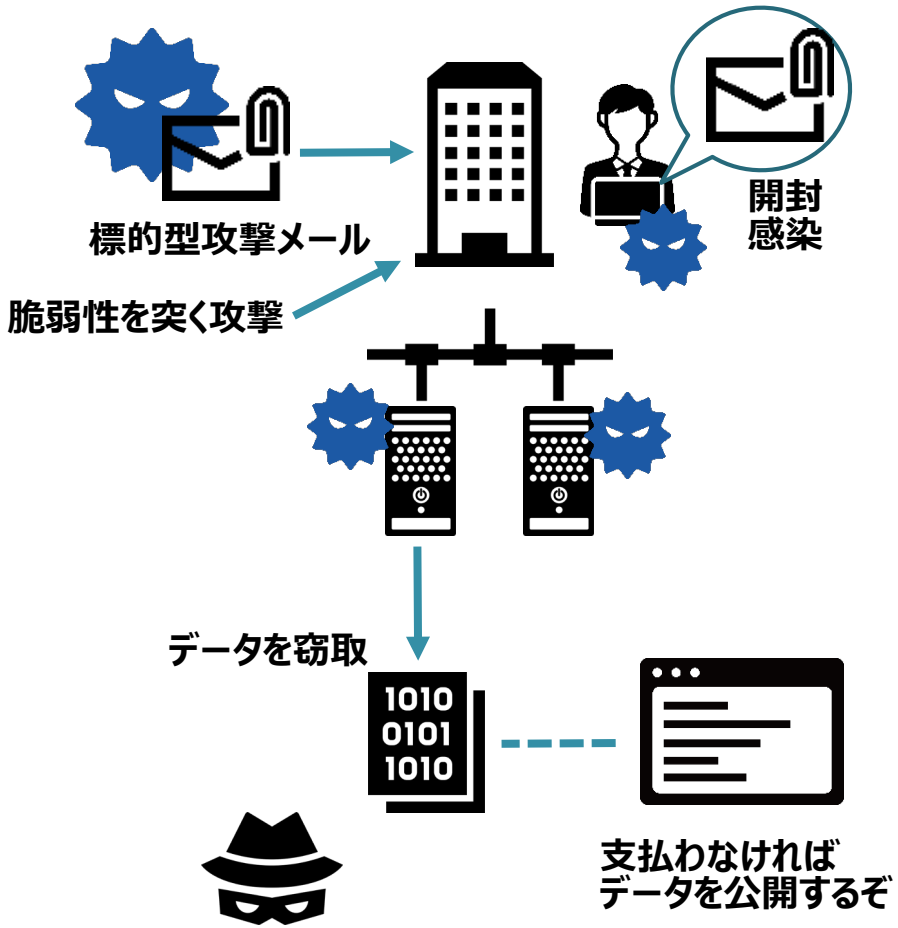
二重の脅迫

「二重の脅迫」とは、ランサムウェアにより暗号化したデータを復旧するための身代金要求に加え、暗号化する前にデータを窃取しておき、「支払わなければデータを公開する」などと二重に脅迫する攻撃方法です。

リークサイト（LOCKBIT3.0）

※一部モザイク処理をしています。





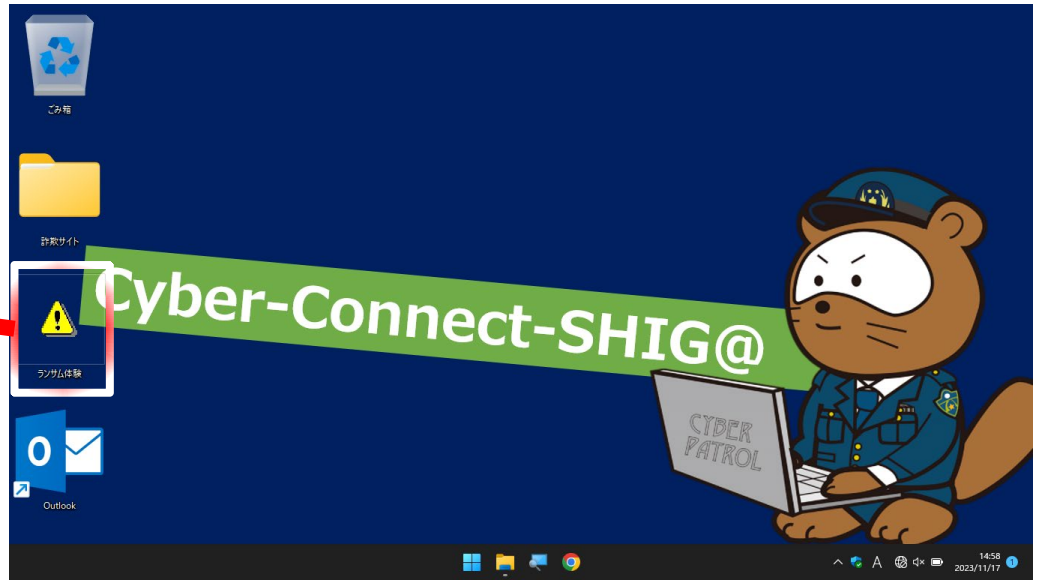
【ランサムウェア攻撃のビジネス化】
ランサムウェアは、一部の犯罪者において「ビジネス」化しています。ダークWebでウイルスやノウハウが販売されており、初心者やスキルが低い犯罪者も関与できるように設計されています。

ランサムウェア（LOCKBIT3.0）の感染

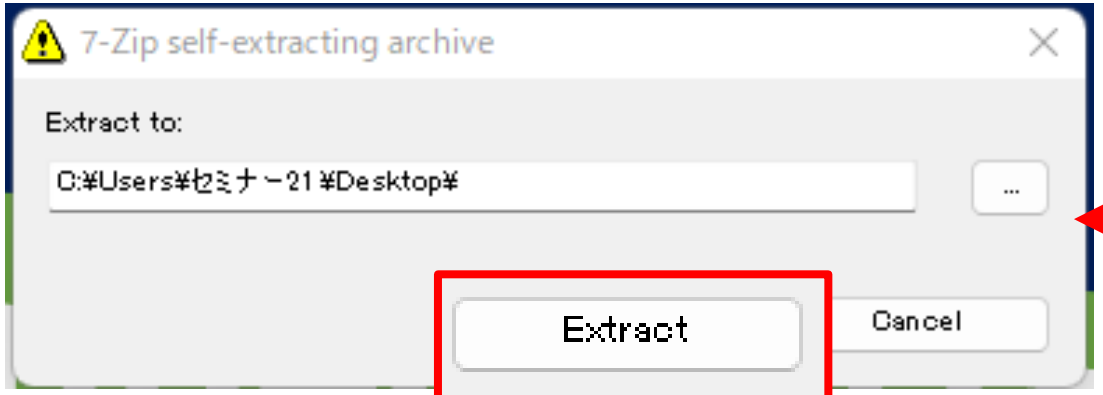
ランサムウェア（LOCKBIT3.0）の感染を体験してみましょう。

1. デスクトップにある「ランサム体験」をダブルクリックで開いてください。

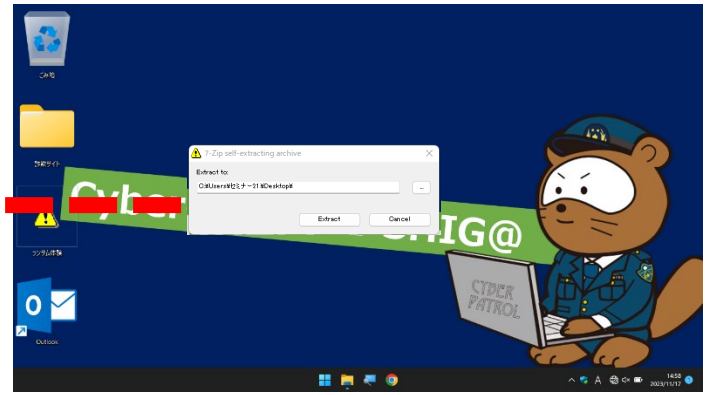
ダブルクリック



2. 「7-Zip self-extracting archive」が開きますので、「Extract」を押してください。



シングルクリック



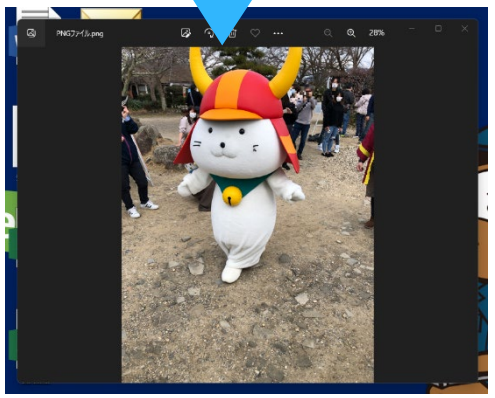
ランサムウェア（LOCKBIT3.0）の感染

3．デスクトップに、エクセルやJPEG等のファイルが作成されます。

それぞれのファイルの中身を確認してみてください。
感染前は、すべてのファイルを見ることができます。

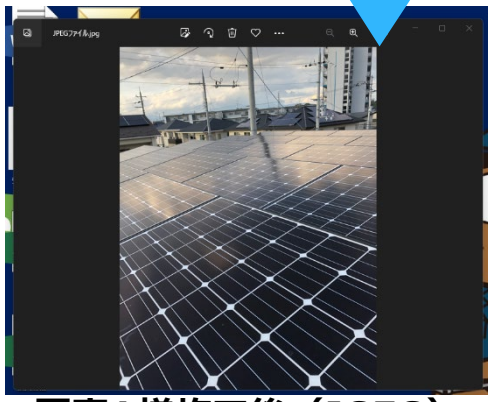
例（デモファイル）

プライベート

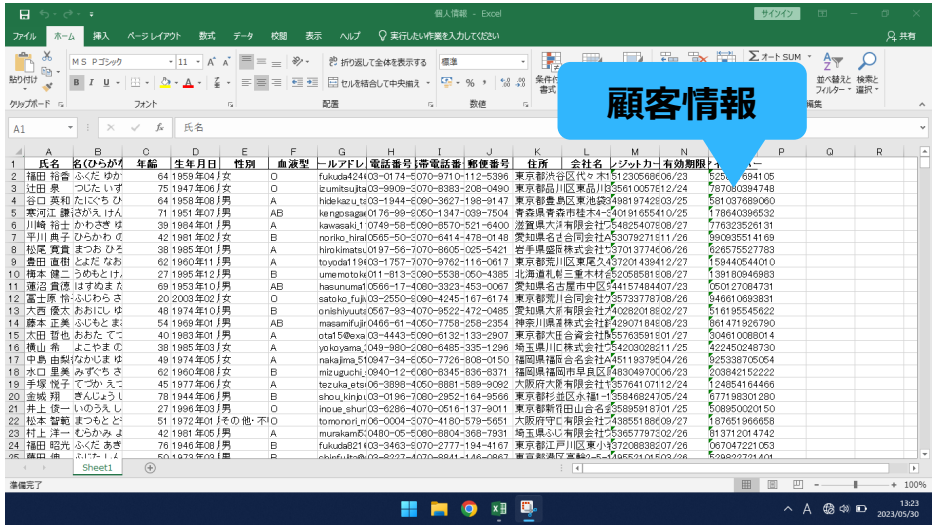


彦根旅行（PNGファイル）

施工後



写真A様施工後（JGEG）



顧客情報

エクセルファイル

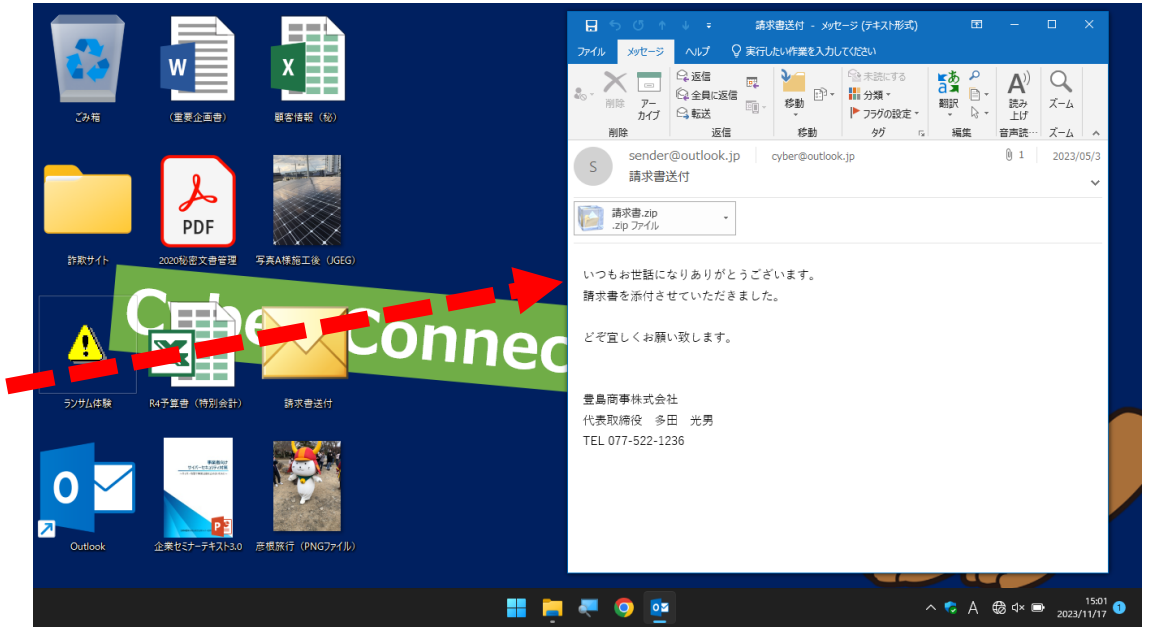
※サンプルです

ランサムウェア（LOCKBIT3.0）の感染

4．デスクトップにある「請求書送付」というメールをダブルクリックで開いてください。

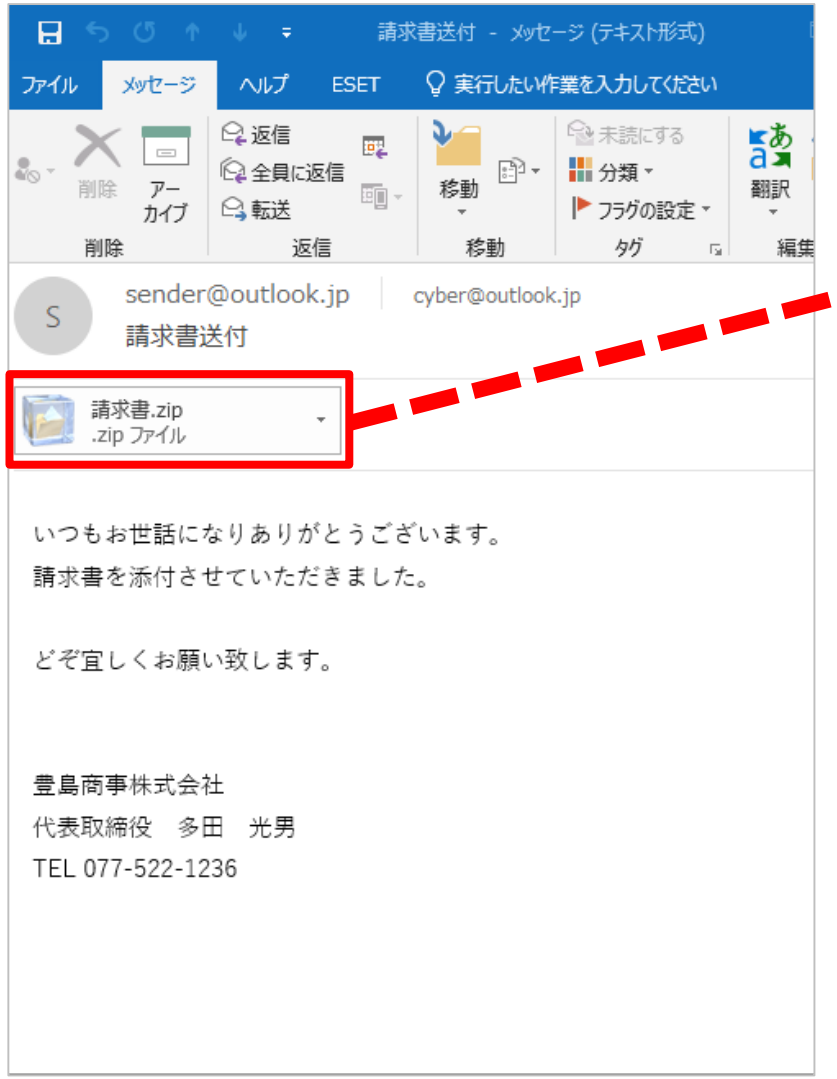
ダブルクリック

メールが開きます。

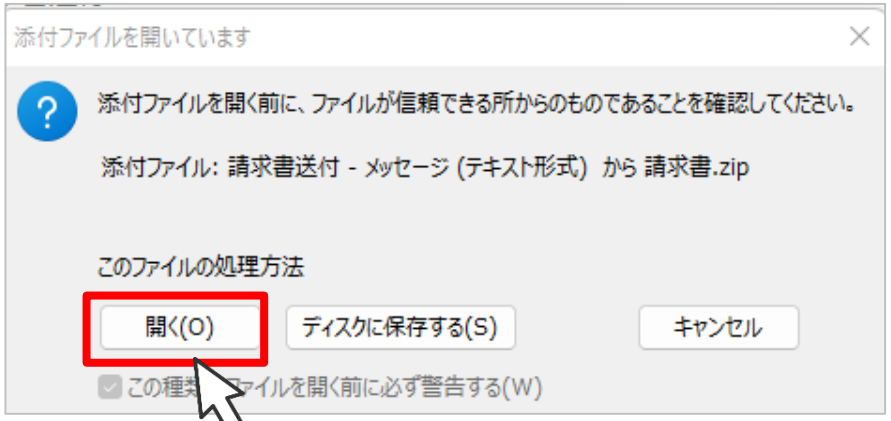


ランサムウェア（LOCKBIT3.0）の感染

5. 添付ファイル「請求書.zip」をダブルクリックで開いて、「開く」を押してください。



ダブルクリック

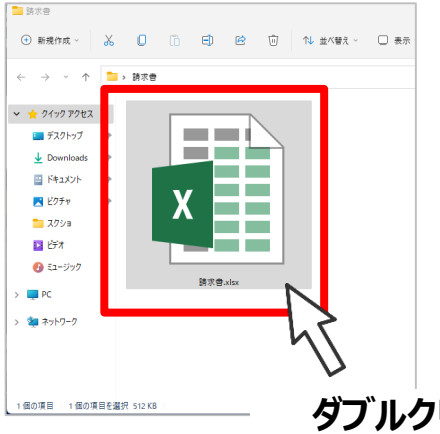


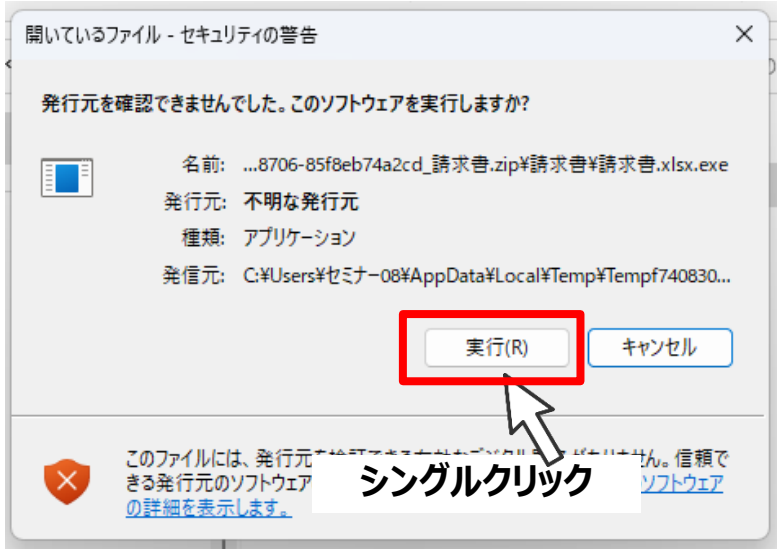
シングルクリック

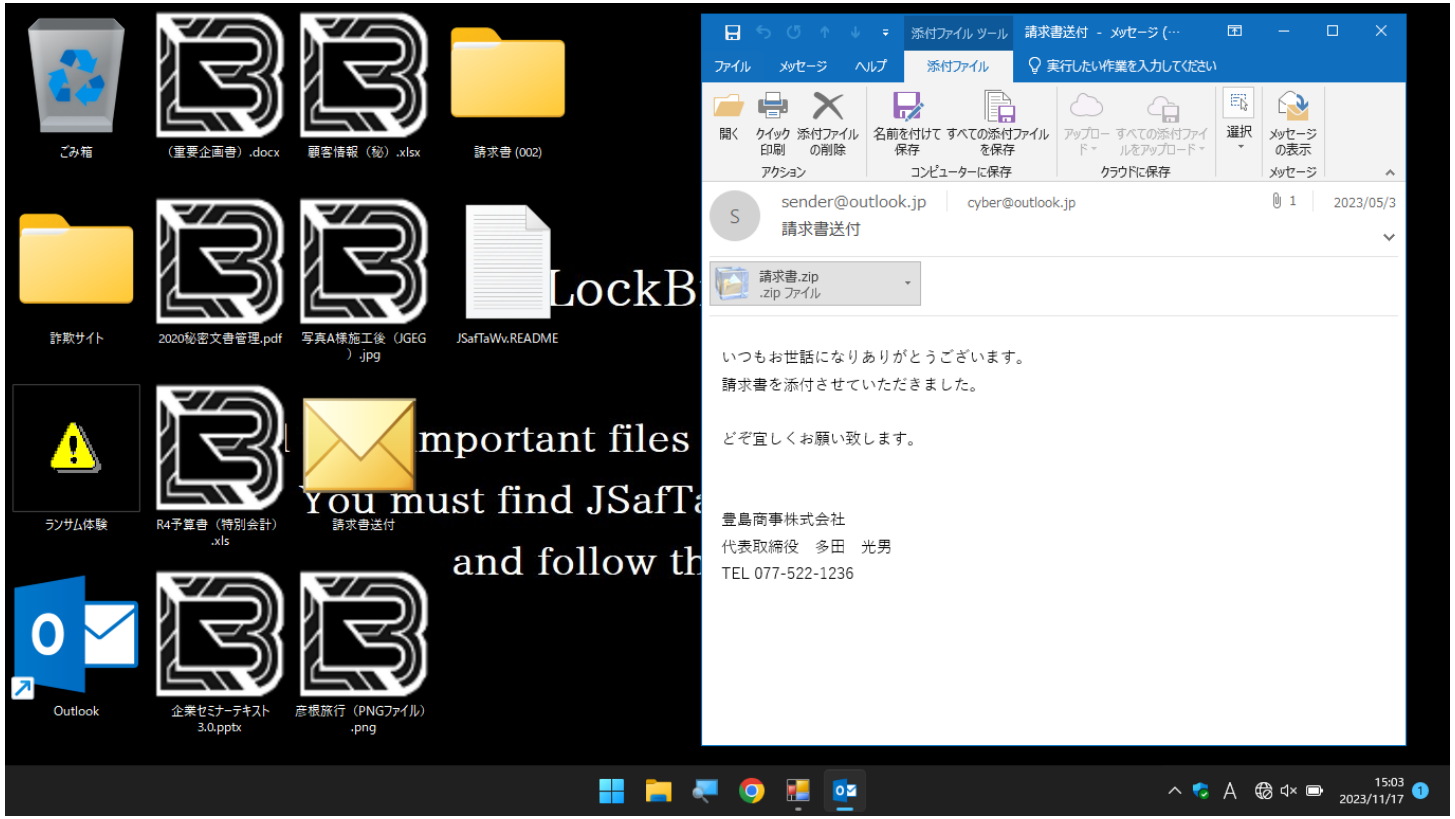
デスクトップに「請求書」フォルダが作成されます。

ランサムウェア（LOCKBIT3.0）の感染

6. 請求書のフォルダを開いて「請求書.xlsx」をダブルクリックしてください。
「セキュリティの警告」が表示される場合がありますが、実行を押してください。（普段は絶対にキャンセルを押してください。）



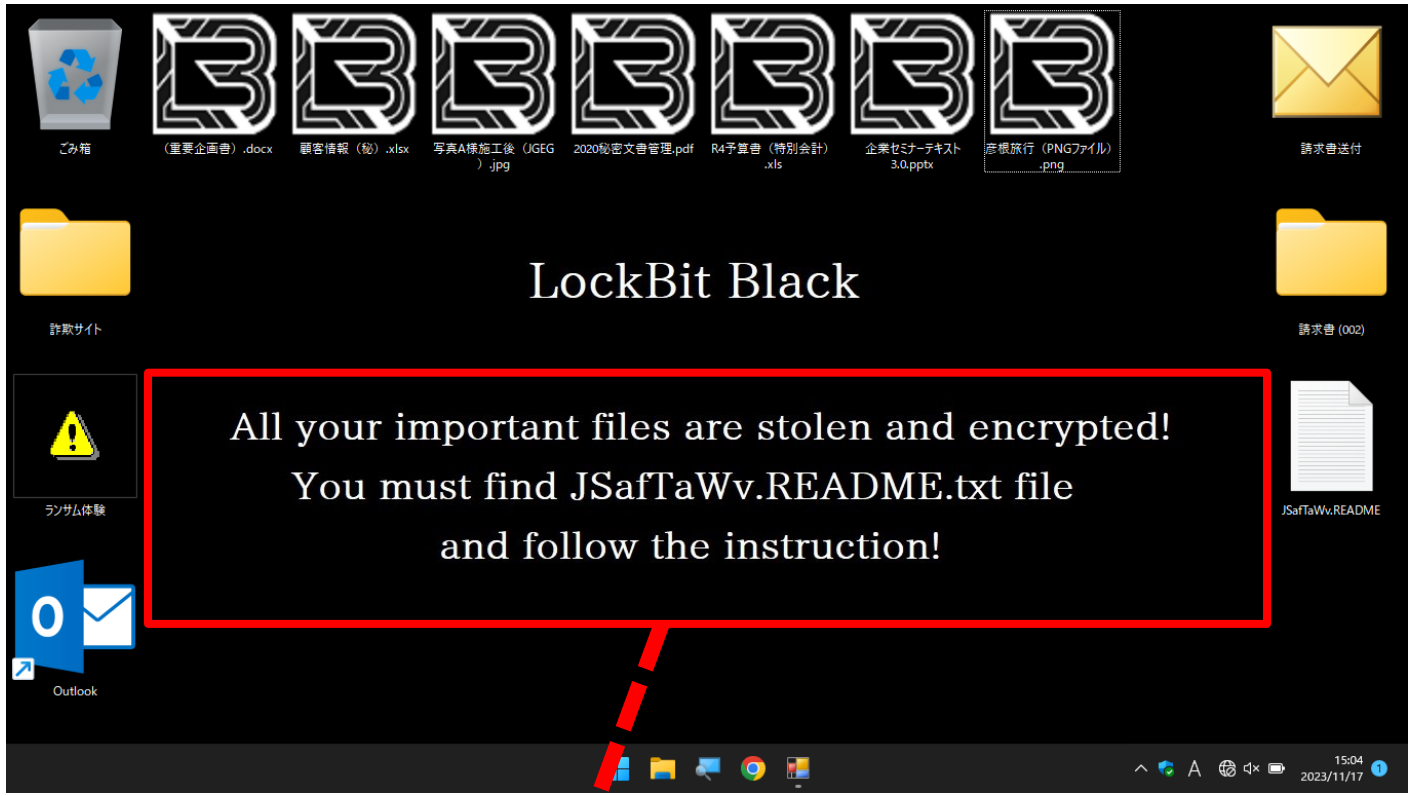




セキュリティの警告を無視して実行を押すと、不正プログラムが実行されデスクトップ画面が変わります。

ランサムウェア（LOCKBIT3.0）の感染

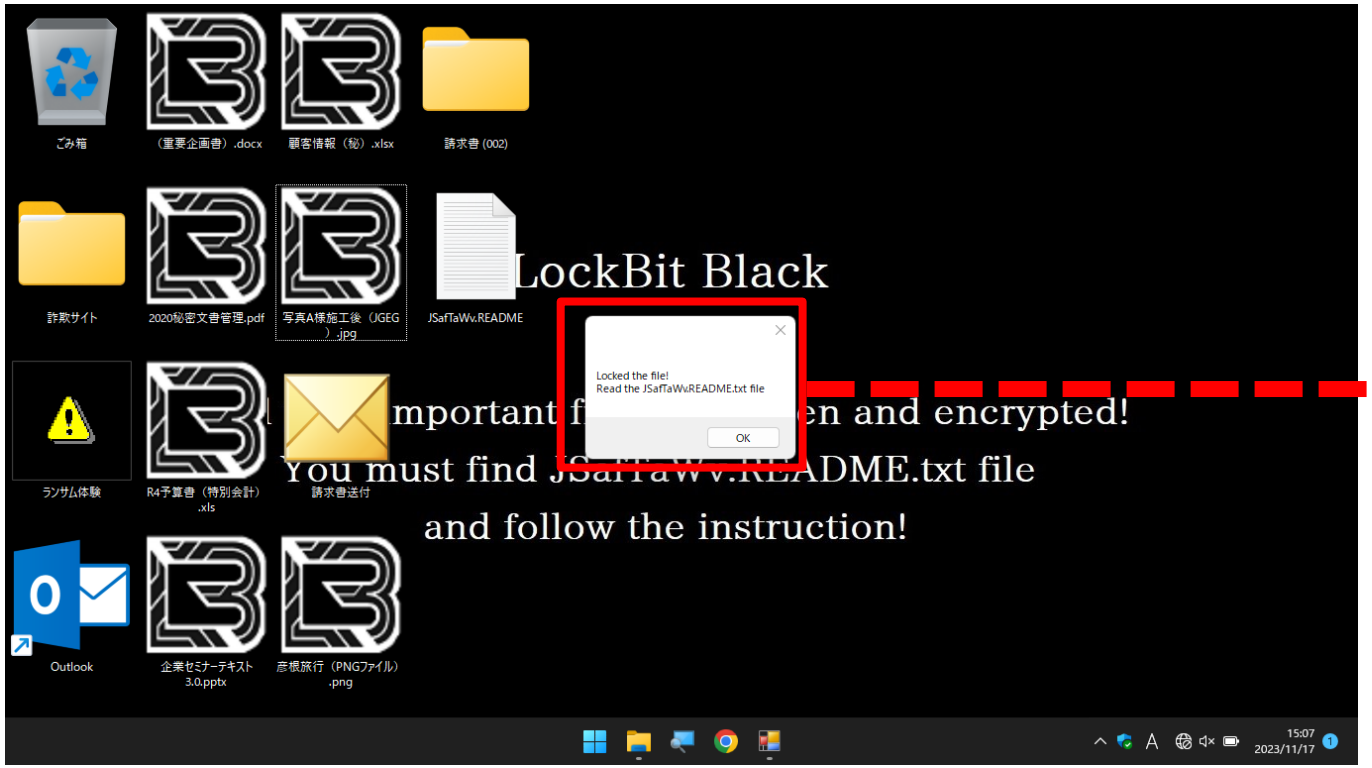
デスクトップに保存したファイルが「B」のアイコンに変わり、デスクトップには「ファイルは盗んだうえ、暗号化した」とのメッセージが表示されます。（デスクトップのメッセージが見やすいようにアイコンの位置を変えています。）

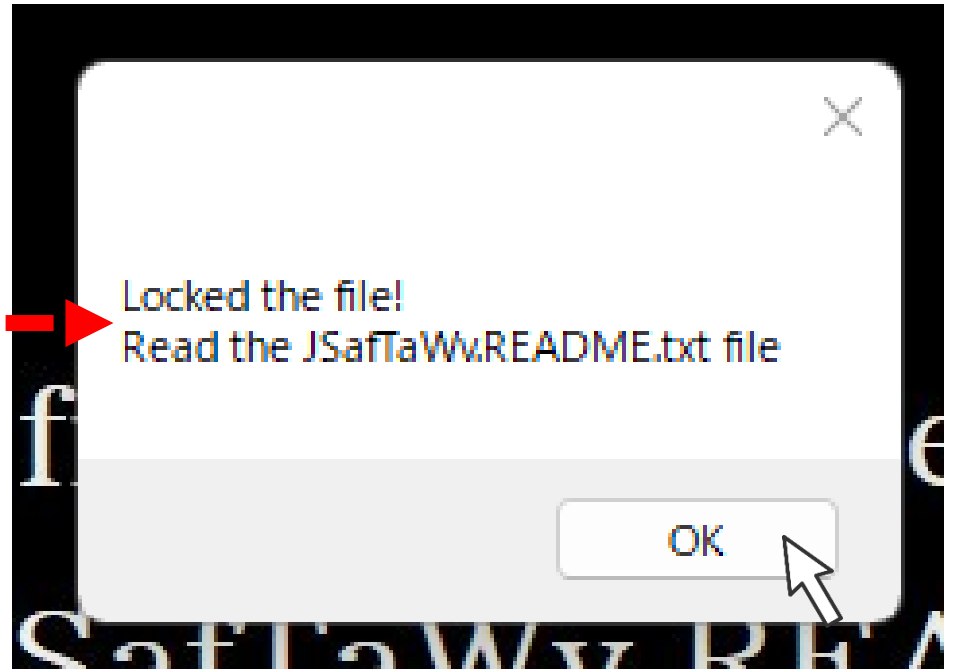


和訳
重要なファイルは、全て盗まれ、暗号化されています！
JSafTaWv.README.txtを見つけて、その指示に従わなければなりません！

ランサムウェア（LOCKBIT3.0）の感染

7.「B」のアイコン（顧客情報、彦根旅行等どれでもいい）のファイルをダブルクリックで開いてみてください。
「ロックされている」というメッセージが表示され、開くことができません。



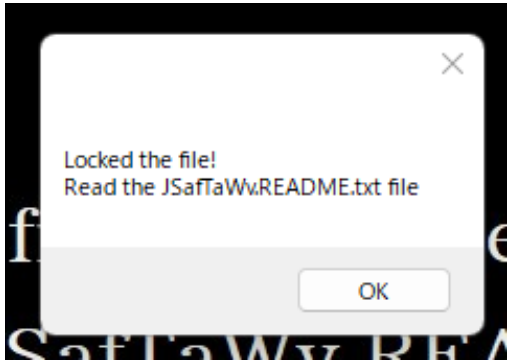


「ファイルはロックされている。
JSafTaWv.README.txtを読め」とのメッセージが表示され、
ファイルを開くことはできなくなりました。

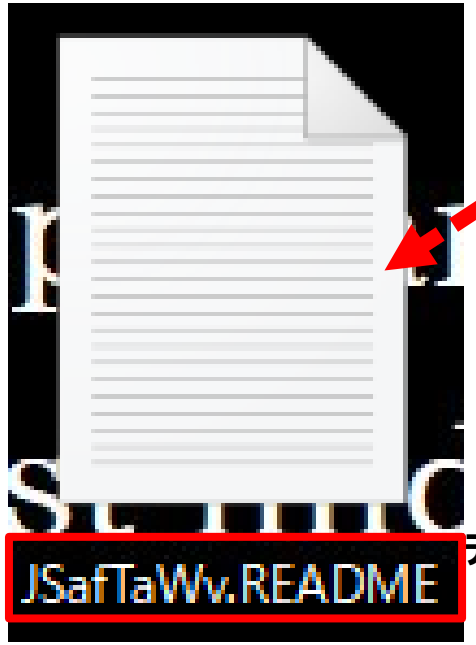
ダブルクリック

ランサムウェア（LOCKBIT3.0）の感染

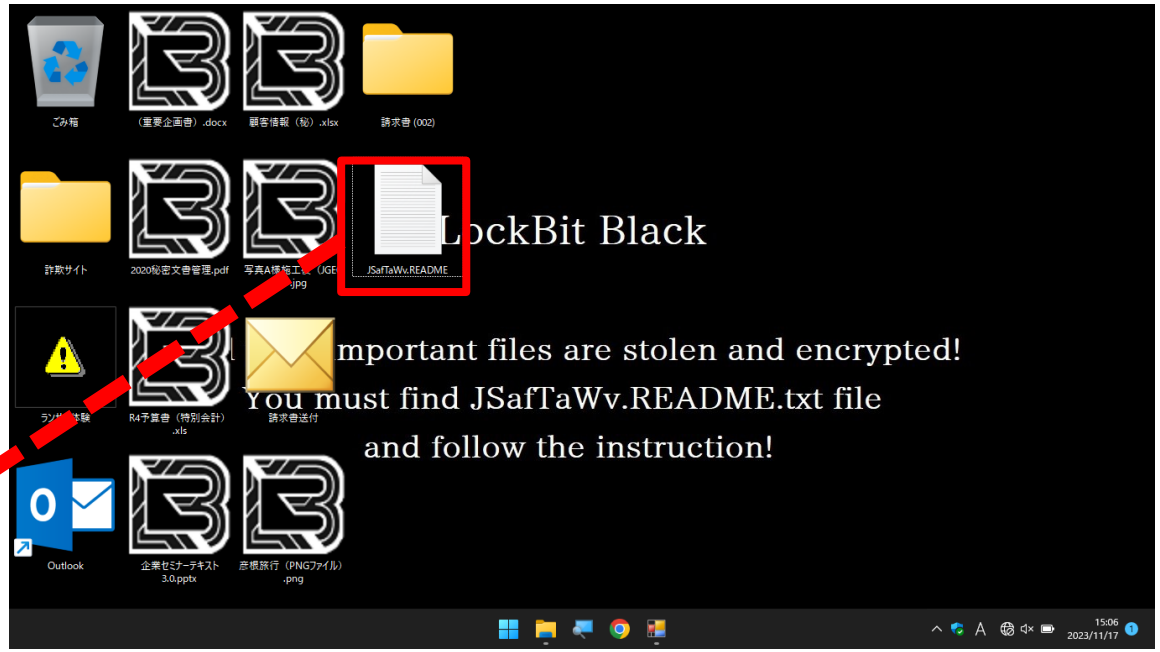
8.「JSafTaWv.README.txt 」ファイルは、デスクトップにありますので、ダブルクリックで開いてください。



「ファイルはロックされている。JSafTaWv.README.txtを読め」とのメッセージが表示されます。

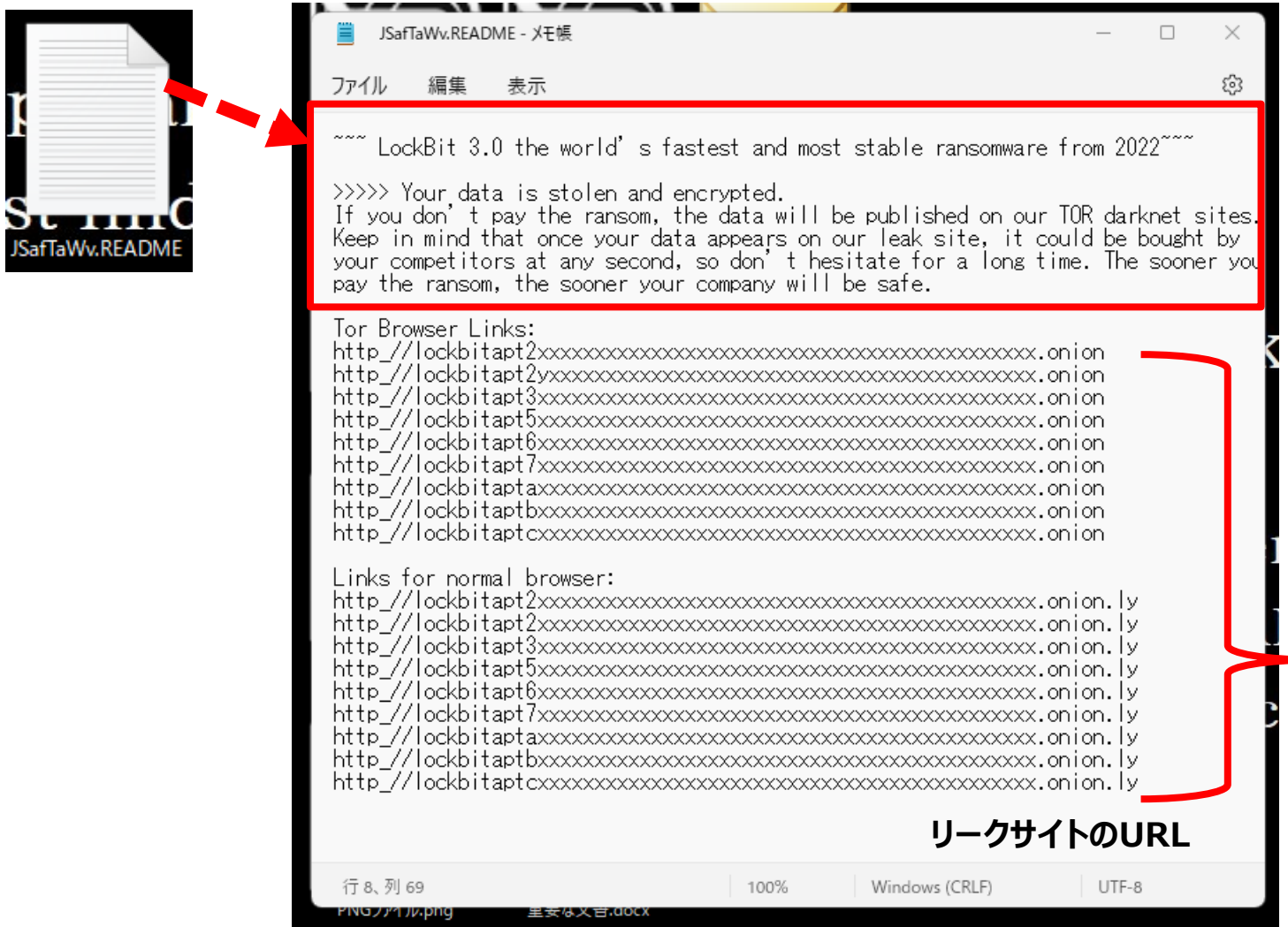


テキストファイルをダブルクリック



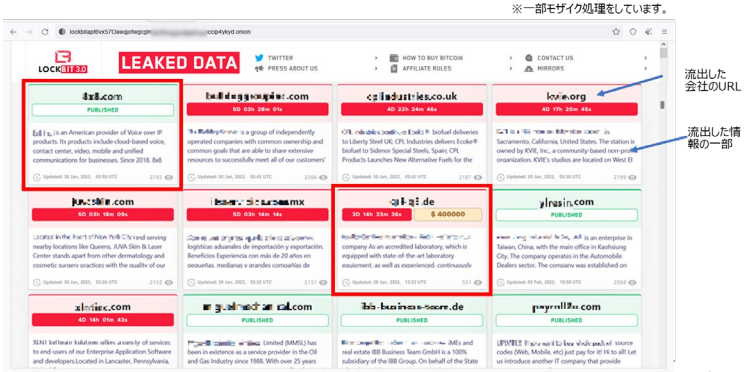
ランサムウェア（LOCKBIT3.0）の感染

9.「JSafTaWv.README.txt 」ファイルは、「ランサムノート」と呼ばれるファイルで、「要求に従わなければ、盗んだ情報を公表する」などの脅迫文が記載されています。



和訳
~~~ LockBit 3.0 は 2022 年から登場する世界最速で安定したランサムウェア~~~

>>>>> あなたのデータが盗まれ、暗号化されます。
身代金を支払わない場合、データは私たちのTORダークネットサイトで公開されます。あなたのデータが私たちのリークサイトに掲載されると、いつ競合他社に買われてもおかしくないので、長い間躊躇しないように留意してください。身代金を支払うのが早ければ早いほど、あなたの会社は安全になるのです。


~~~

事例：ランサムウェア、従業員情報の流出等（滋賀県内）

概要：ある朝、社員が出勤してタイムカードを押したところエラーとなり、時間が記録されない事案が発生。調査結果によると、データベースに記録されていた社員情報と出退勤時間データが全て消えていたことが判明。サーバには、英語で「元に戻してほしければ0.1ビットコインをXXXXに送金しろ」というメッセージが残されていた。削除された社員情報は、氏名、社員番号等
原因：不正アクセス
→パスワードリスト型攻撃
（デフォルトのパスワード）
被害：社員情報の削除及び流出
その他：顧客情報の流出はなし。
・・・監査ログなし→被疑者追跡できず。

初期設定時のパスワードは変更してください。

概要：量販店のショッピングサイトが改ざんされ、顧客情報が流出したおそれあり。
原因：ショッピングサイトを作成するソフトウェアの脆弱性が悪用された。
被害：顧客情報数百件
ウェブサイトの停止

ソフトウェアの脆弱性発見時は更新が必要です。

概要：食品加工会社のサーバ内のファイルが暗号化され、1000ビットコインを要求された。
原因：セキュリティ対策の不備を突かれて、内部のファイルサーバにアクセスされたもの。
被害：ファイルが暗号化されたことによる業務停止

セキュリティ設定に不備がないかを確認してください。

滋賀県内においてもサイバー攻撃による被害が発生しています。

ランサムウェア（まとめ）

- ランサムウェアに感染すると、パソコンのファイルが全て暗号化され、全く使えなくなります。
- また、感染前に重要データが盗まれている場合は、リークサイトで公開されるなどの脅迫を受けることがあります。
- 感染は、ネットワークでつながっているパソコンやサーバに広がるおそれがあります。

【ランサムウェア対策】

- ウイルス対策ソフトの導入と更新
- OSやソフトウェアの更新（VPN等機器の更新）
- 外部との通信の監視
- 重要データのバックアップ
  （同一ネットワーク内のバックアップは避ける）
- メールの添付ファイルに対する警戒
  （標的型メール攻撃によるウイルス感染を防ぐ）

バックアップの3-2-1ルール

①データを３つ作成

運用データ…1つ
バックアップ…2つ

②バックアップを２つの媒体で保存

バックアップサーバ…1つ
外部記録媒体等…1つ

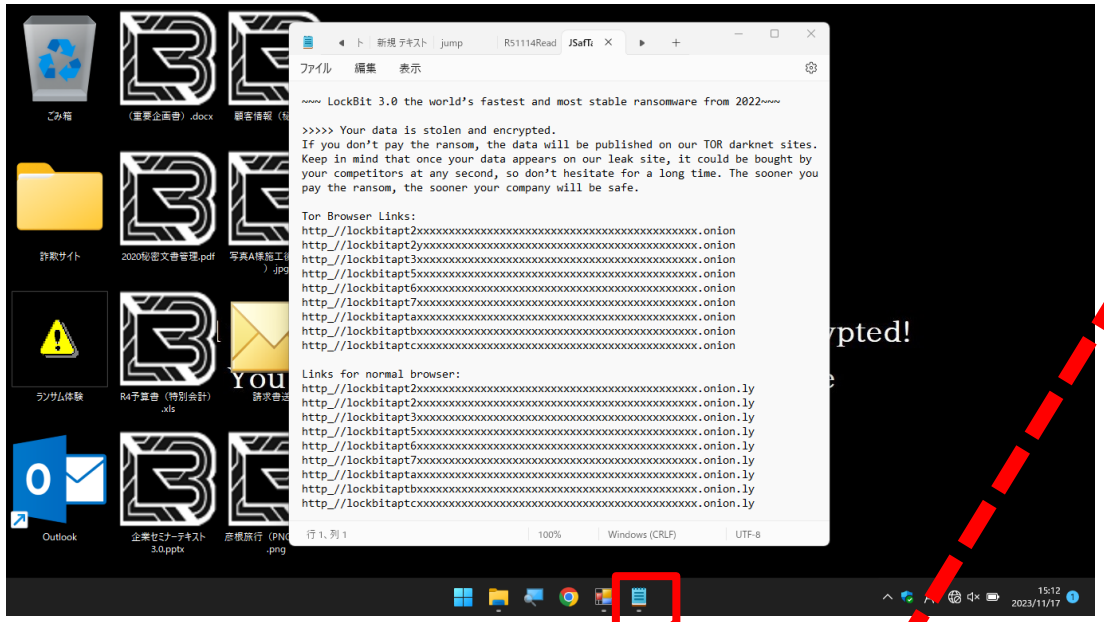
③１つの別の場所で保存

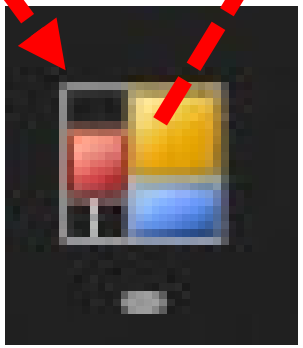
遠隔地…１つ
（物理的に離れた場所）

**万が一、感染してしまった場合は、すぐにネットワークを切断してください。
電源は切らないでください。**

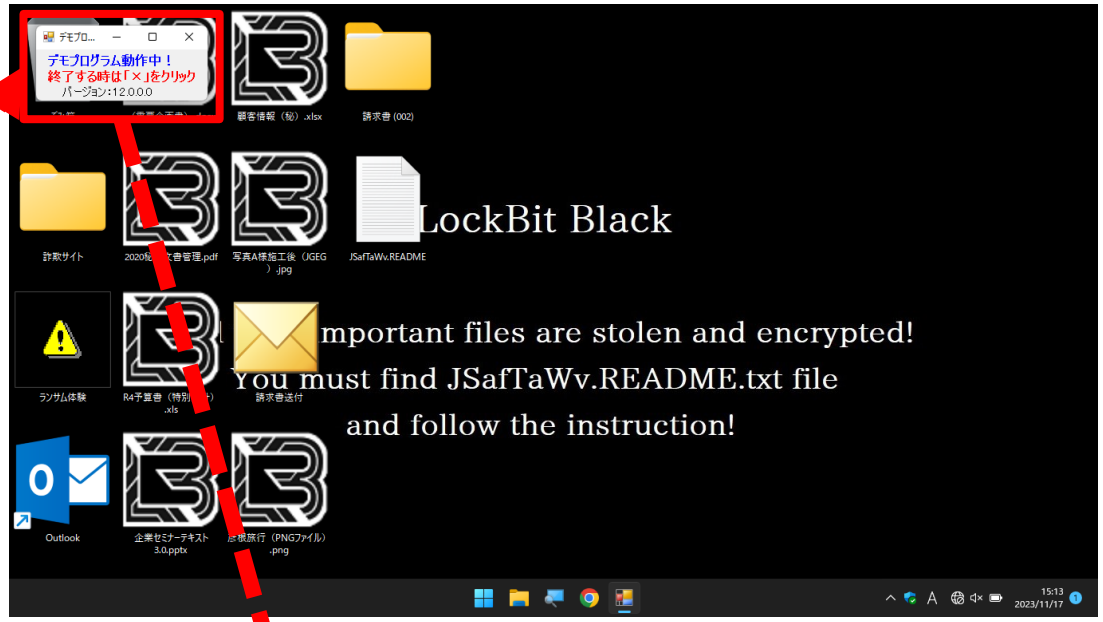
ランサムウェア（LOCKBIT3.0）の感染

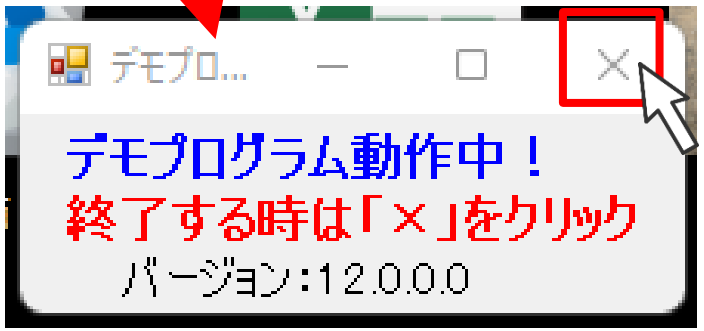
10.最後に、画面を元に戻します。タスクバーにある「赤、黄、青の四角のアイコン」をクリックして、「デモプログラム動作中！」のメッセージが表示されたら、「×」を押してください。





シングルクリック

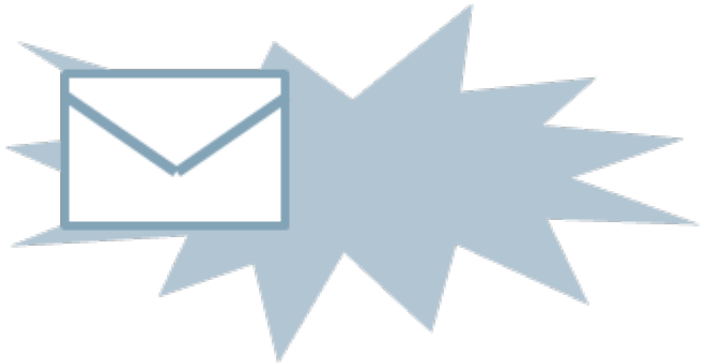




「×」ボタンを押すと元に戻ります。

標的型メール攻撃とは？

特定の企業等を狙って、
業務に関係するような内容を装って
ウイルス添付メールを送信し、
受信したコンピュータをウイルスに感染させ、
情報窃取などを行う攻撃



サプライチェーンを利用して、取引先や業務提携先の
企業が攻撃対象となる場合もあります。

滋賀県内で発生した事例（メールの内容）

［送信者］■■■社　■■■■（氏名）＜●●●@●●●.com＞
［件名］請求書送付のお願い
［宛先］○○社　○○さん
［添付］ 請求書2020_08_**.doc(224KB)

［メッセージ］
お世話になっております。

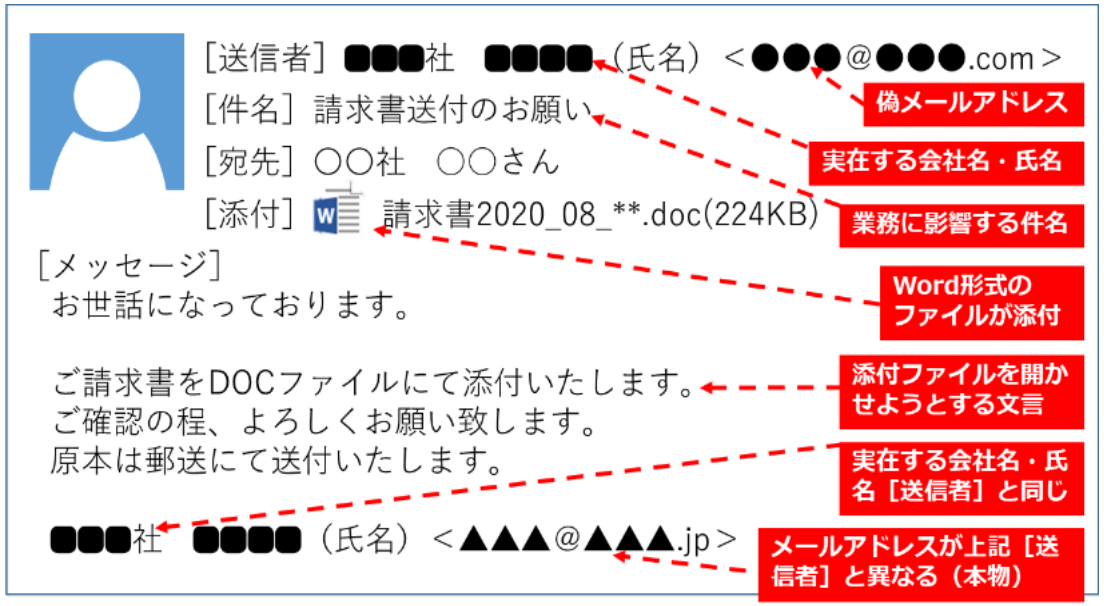
ご請求書をDOCファイルにて添付いたします。
ご確認の程、よろしくお願い致します。
原本は郵送にて送付いたします。

■■■社　■■■■（氏名）＜▲▲▲@▲▲▲.jp＞

「請求書」（Wordファイル）を開封した後、しばらくして顧客、業者等から「変なメールが来た」「ファイルを開いたが何も書いていない」という問い合わせが殺到。
なりすましによるメールと気付き、登録しているメールアドレスの業者に電話で連絡。

滋賀県内で発生した事例（確認ポイント）

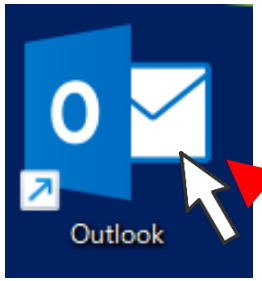
1	送信者が実在するか	送信者の名称を確認してください。 実在する会社名・氏名の場合もあります。
2	件名が業務に影響するものか	攻撃者はマルウェアに感染させるため、業務や興味がありそうなことを件名に入れます。
3	メールアドレスに不審点がないか	送信メールアドレスとメール本文に記載されているメールアドレスが異なっている場合があります。またフリーメールアドレスの場合は、匿名性が高いので攻撃によく利用されます。
4	添付ファイルがあるか	添付ファイルがある場合は、不用意に開かないでください。表示されているアイコンとファイル形式が異なる場合があります。開く前にプロパティでファイル形式を確認してください。 また、ファイルを開く場合は、必ずウイルススキャンをしてください。
5	メール本文に添付ファイルを開かせようとする文言があるか	添付ファイルは開かなければ、マルウェアに感染しません。攻撃者は、メール本文に添付ファイルを開かせるような文言を入れてきます。
6	メール本文にURLがあるか	メール本文に記載されているURLは偽装されている場合がありますので、アクセスしないようにしてください。



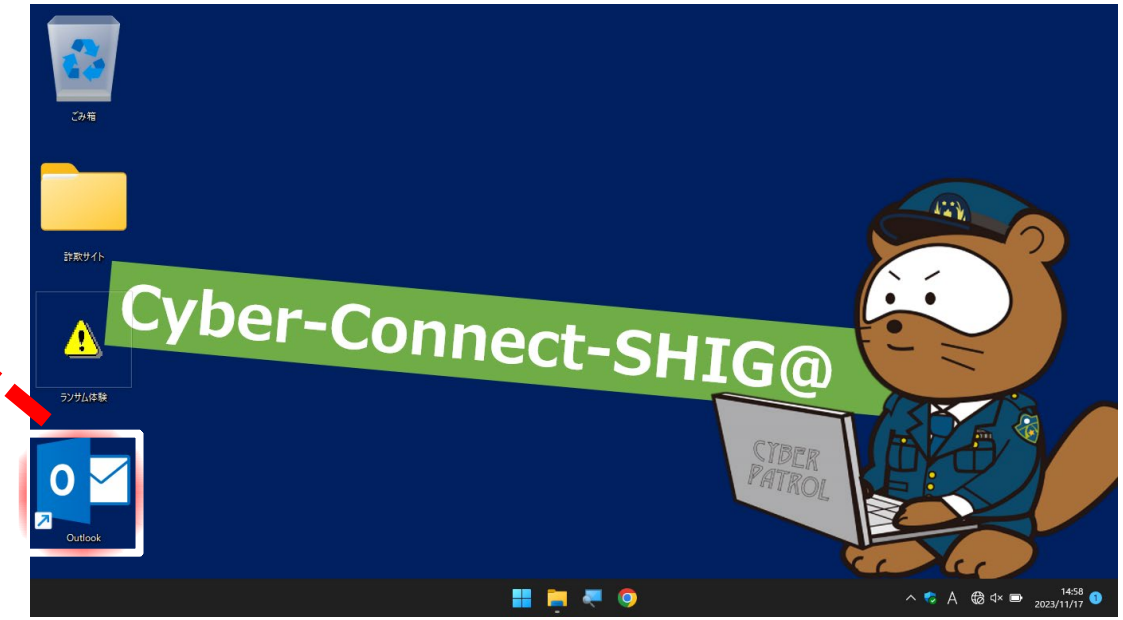
標的型メールの判別

標的型メールを体験してみましょう。

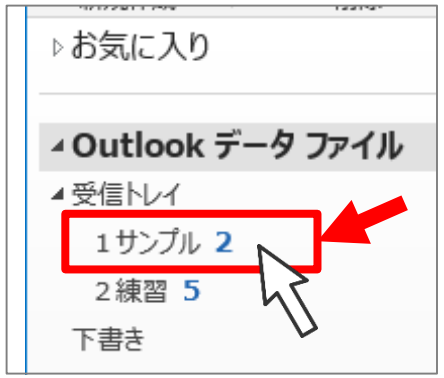
1. デスクトップにあるメールソフト（Outlook）を開いてください。

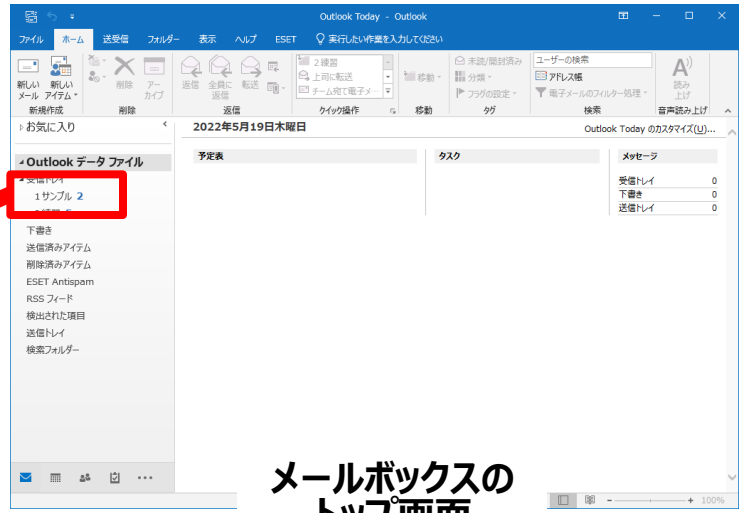


ダブルクリック



2. メールボックスが開きますので、受信トレイの「１サンプル」をクリックしてください。

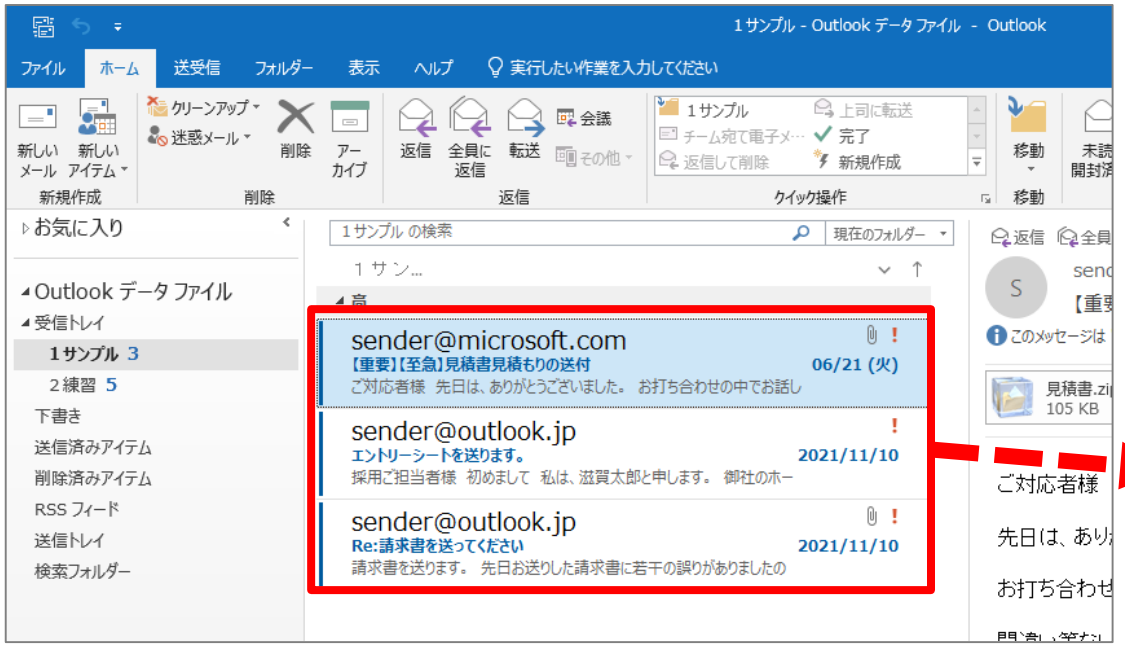




メールボックスのトップ画面

標的型メールの判別（ファイル偽装）

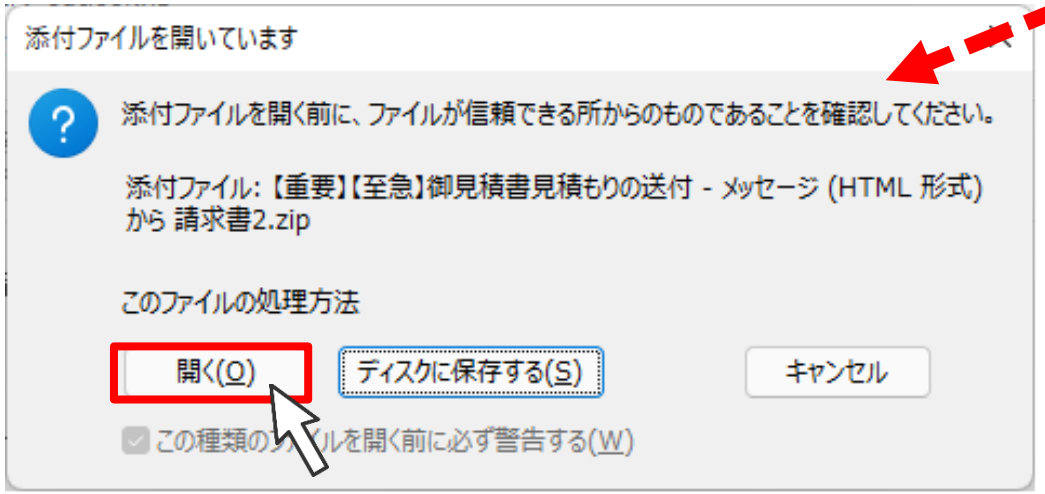
3．3つのメールが受信されますので、順番に開いて確認します。

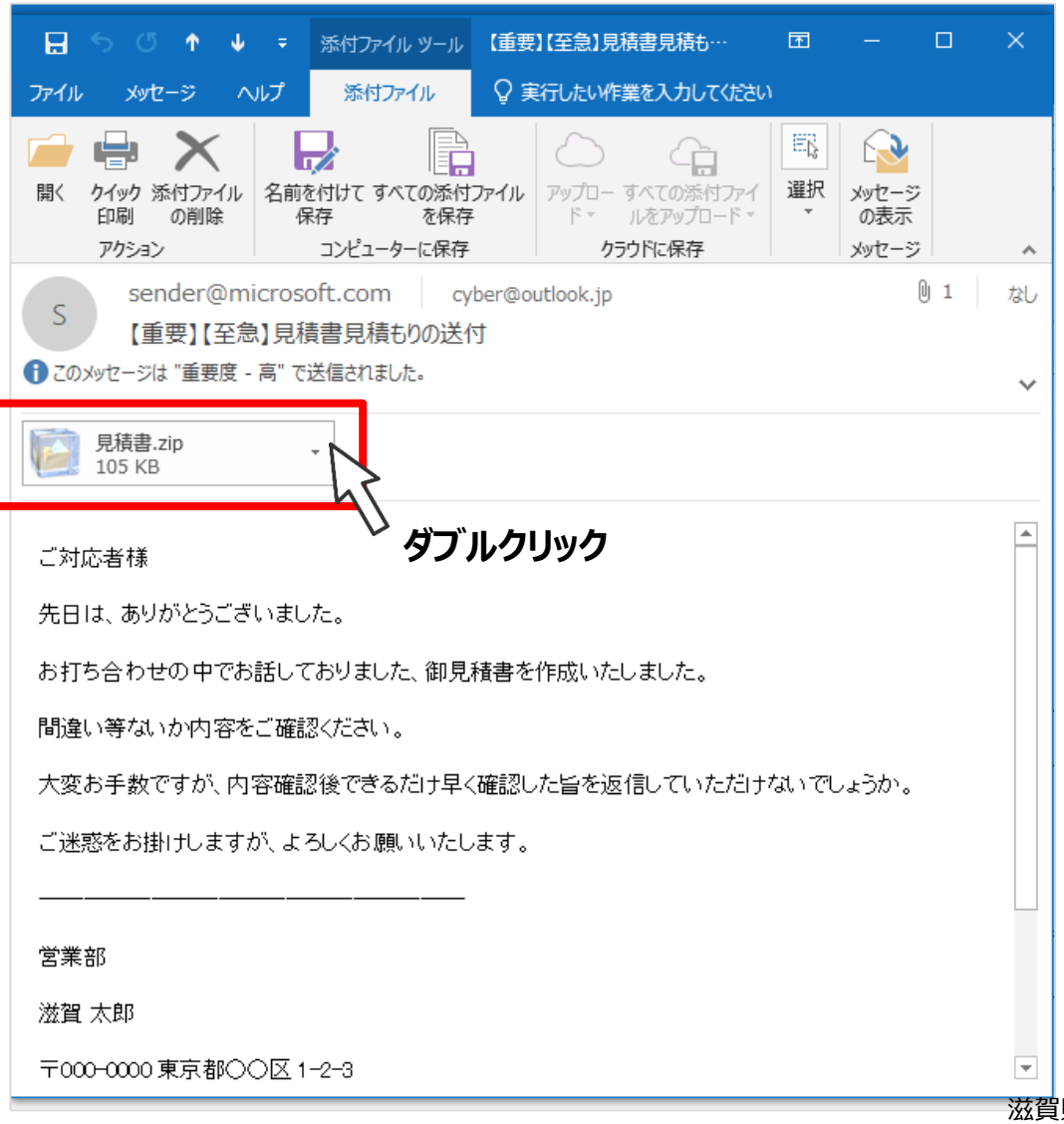


一番上のメールをダブルクリックしてください。

標的型メールの判別（ファイル偽装）

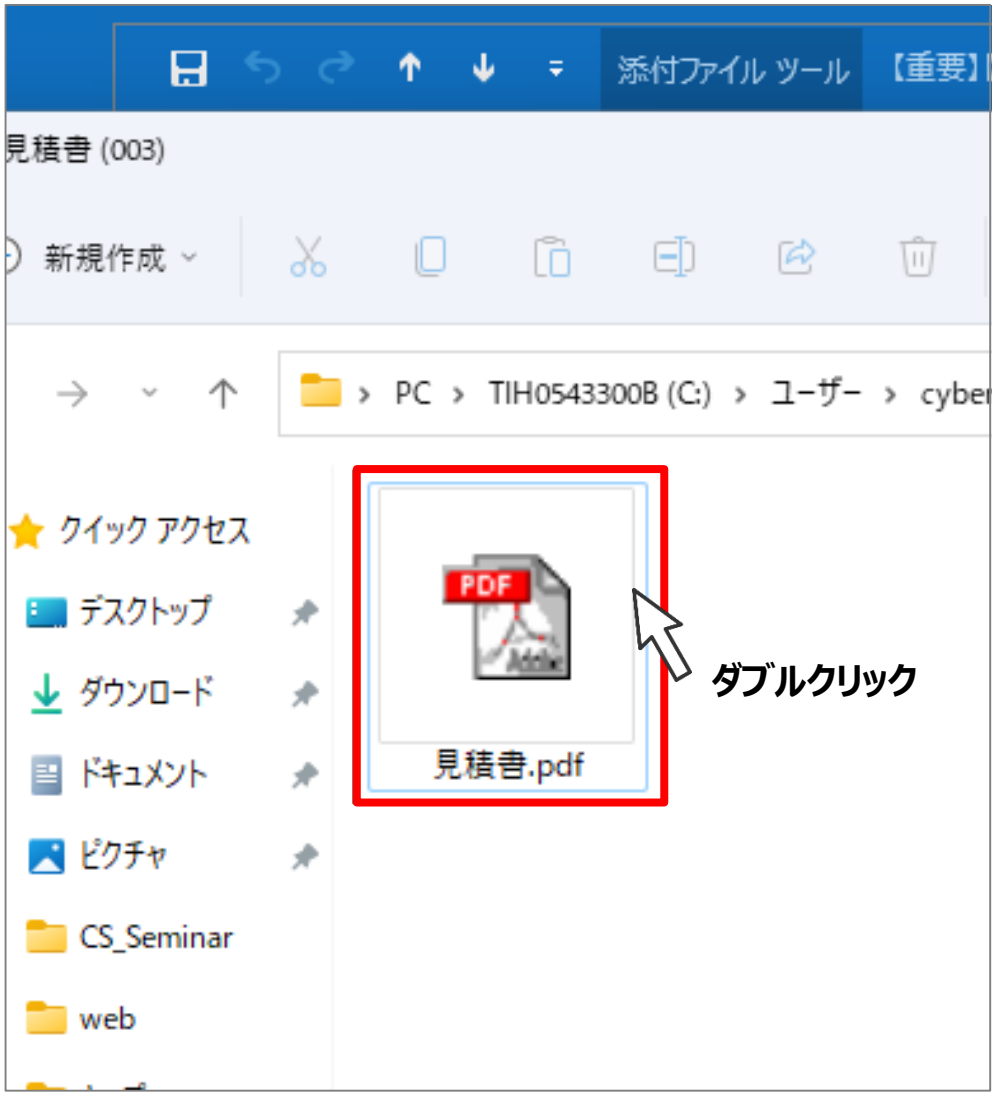
4. 添付ファイルをダブルクリックしてください。「添付ファイルを開いています」というメッセージが開きますので、「開く」を押してください。
（デスクトップにファイルが保存されます。）





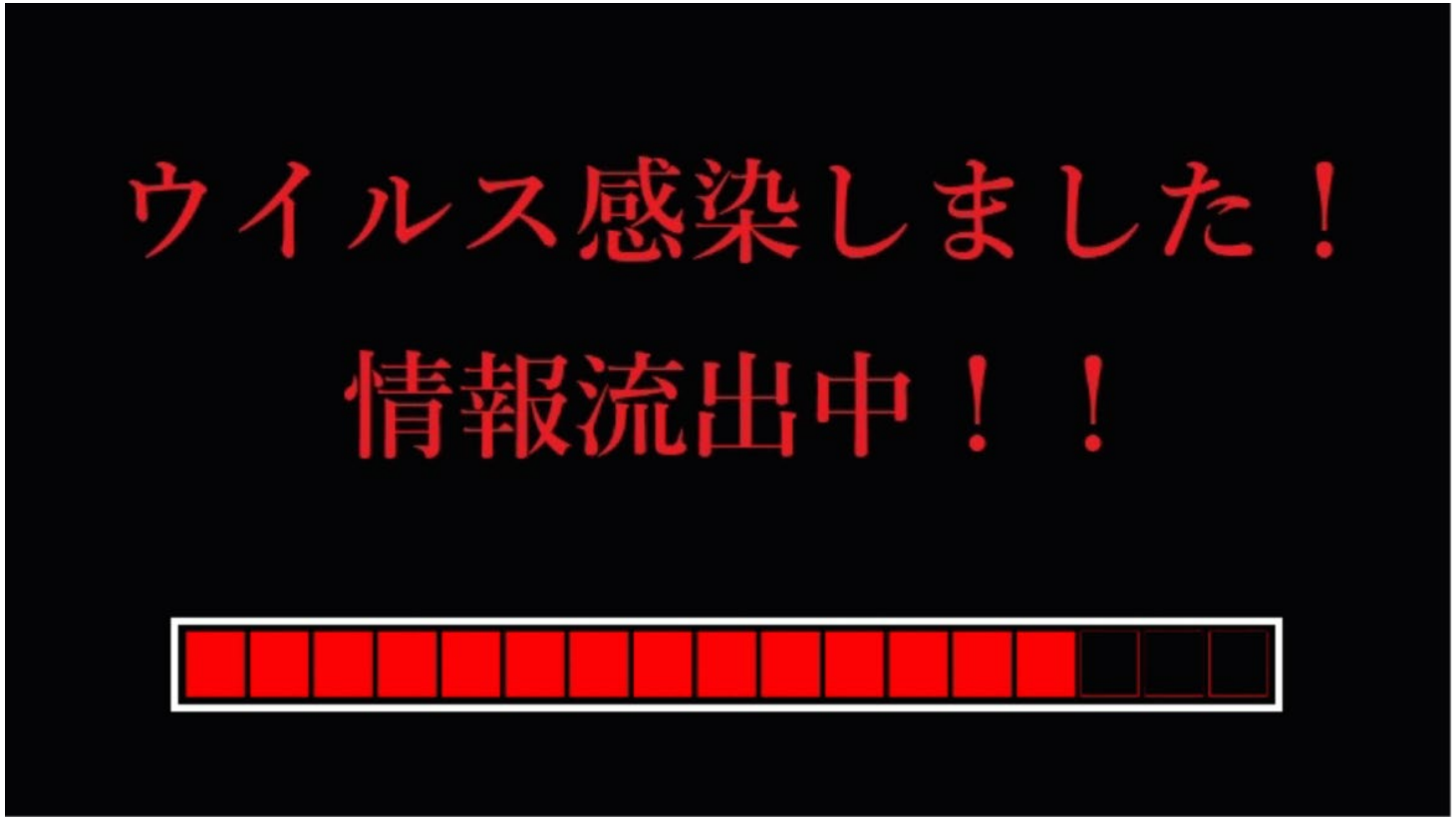
標的型メールの判別（ファイル偽装）

5. フォルダが開き、ファイルが1つ表示されますのでダブルクリックして開いてください。



標的型メールの判別（ファイル偽装）

6.「ウイルス感染しました」と表示されます。



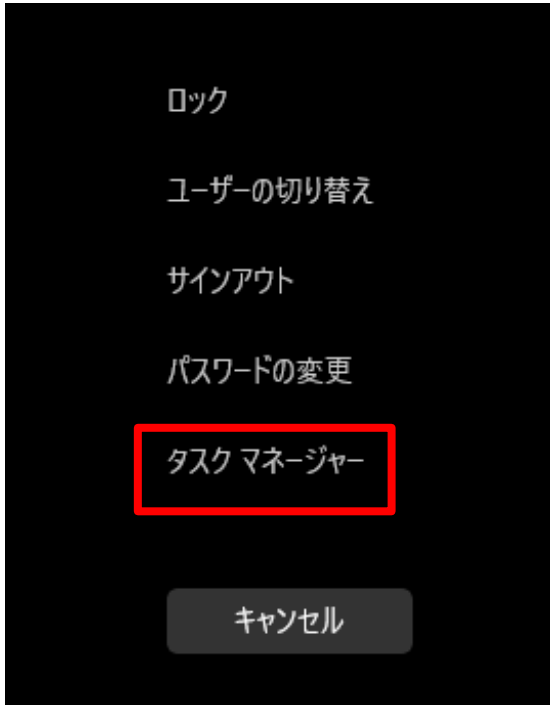
※ウイルス感染したことがわかりやすいようにアニメーションにしています。
多くのウイルス感染は、感染したことがわからないようになっています。

標的型メールの判別（ファイル偽装）

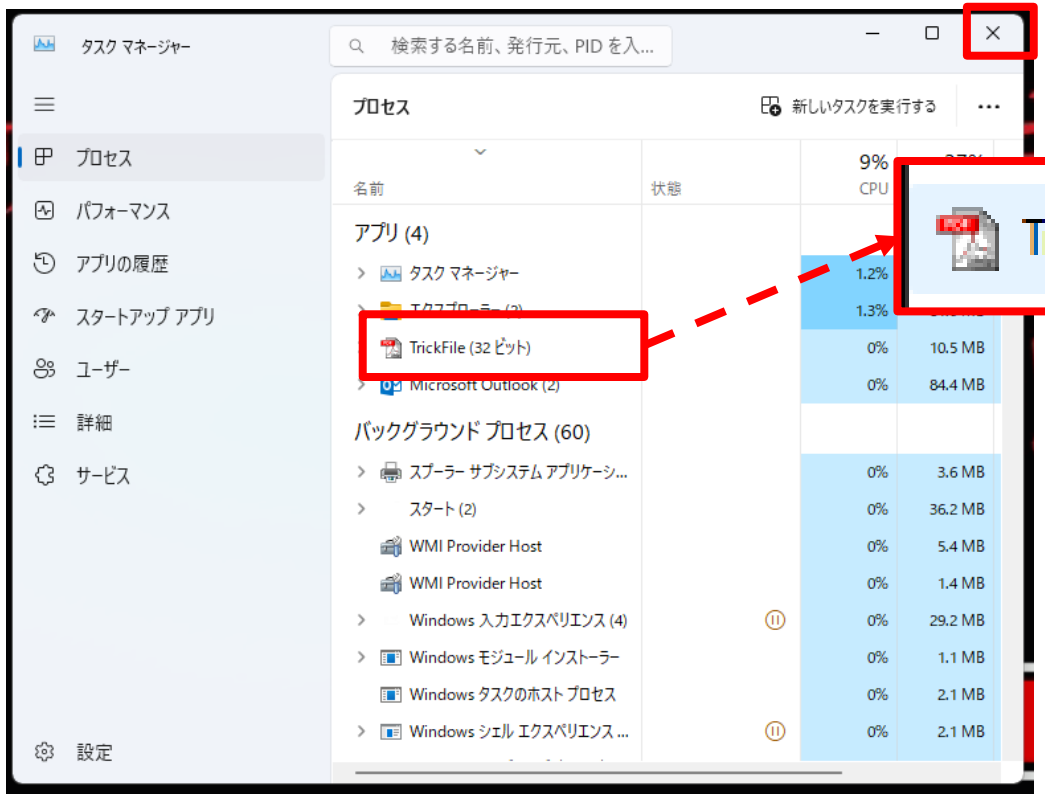
【裏技】一番上のアプリの強制終了
キーボードの「Alt」+「F4」を同時に押すと一番上のウインドウに表示されたアプリが終了できます。

7. 画面を消します。
マウスでは操作できないので、キーボードを使います。

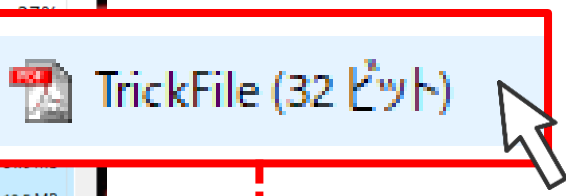
キーボード（ショートカットキー）
「**Alt**」+「**Ctrl**」+「**Delete**」→「タスクマネージャー」を選択



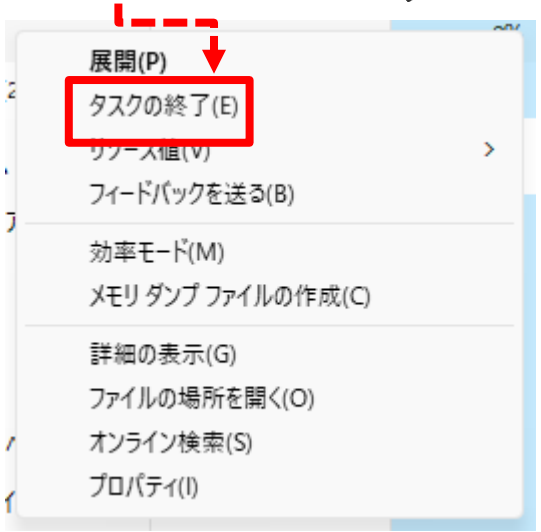
①「Alt」+「Ctrl」+「Delete」→「タスクマネージャー」を選択



**③「×」でタスクマネージャーを終了してください。
Outlookは消さないでください。**



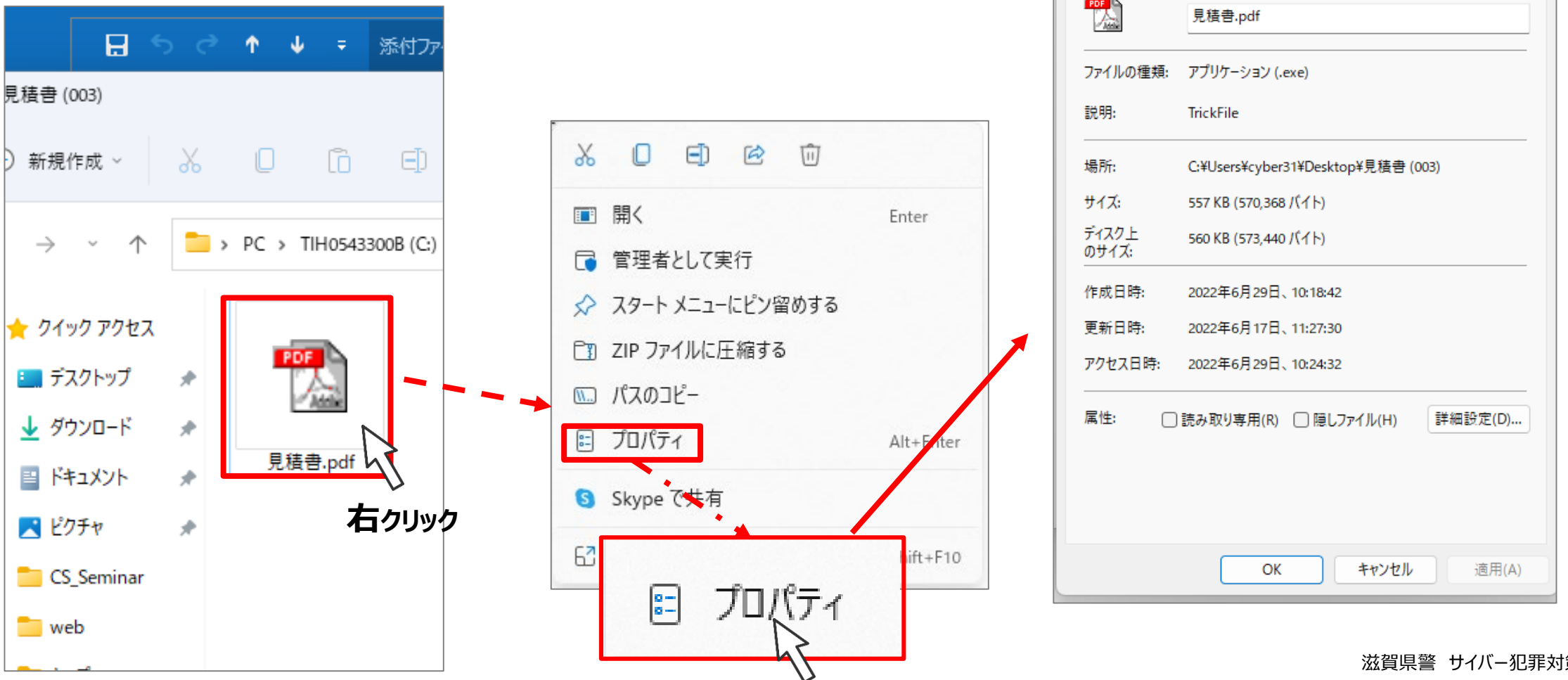
右クリック



②消したいアプリ（TrickFile）を選択して右クリック「タスクの終了」を押す。

標的型メールの判別（ファイル偽装）

8．このファイルは、実行ファイルがPDFファイルに偽装されていました。
ファイルを開く前にプロパティでファイルの形式を確認してください。
（デスクトップにあるファイルを右クリックしてプロパティを見てください）



標的型メールの判別（ファイル偽装）

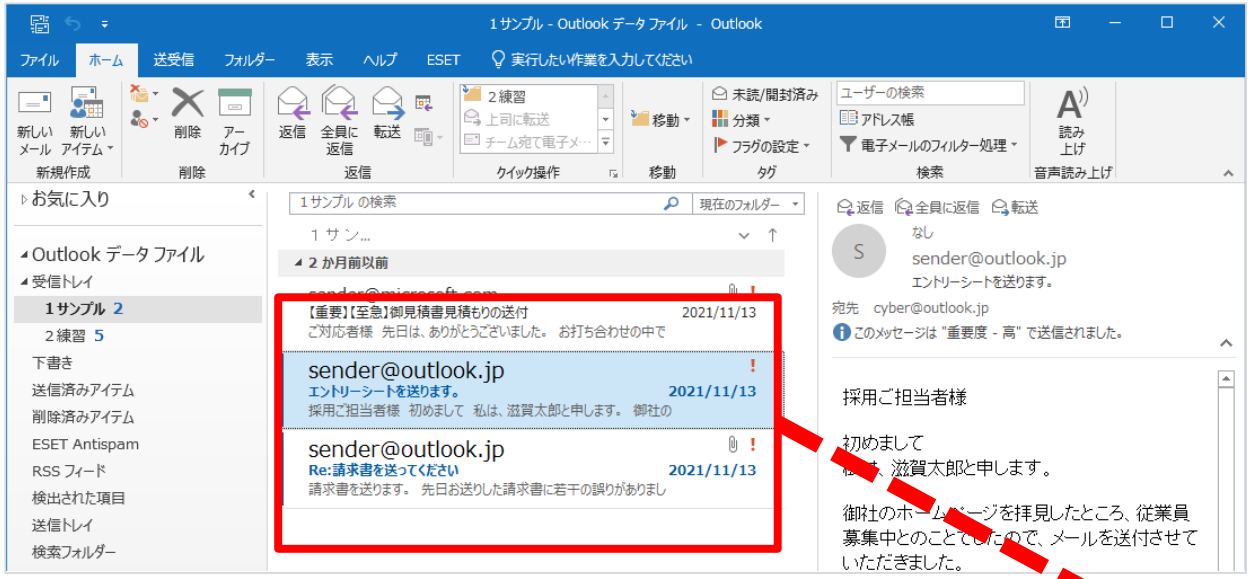
9．プロパティでファイルの形式を確認してください。
「ファイル名の拡張子」と「ファイルの種類」が一致しているかを確認してください。

ファイルの種類が「アプリケーション（.exe）」の場合は、要注意です。

ファイルの種類がPDFではなく、アプリケーション（.exe）となっている。

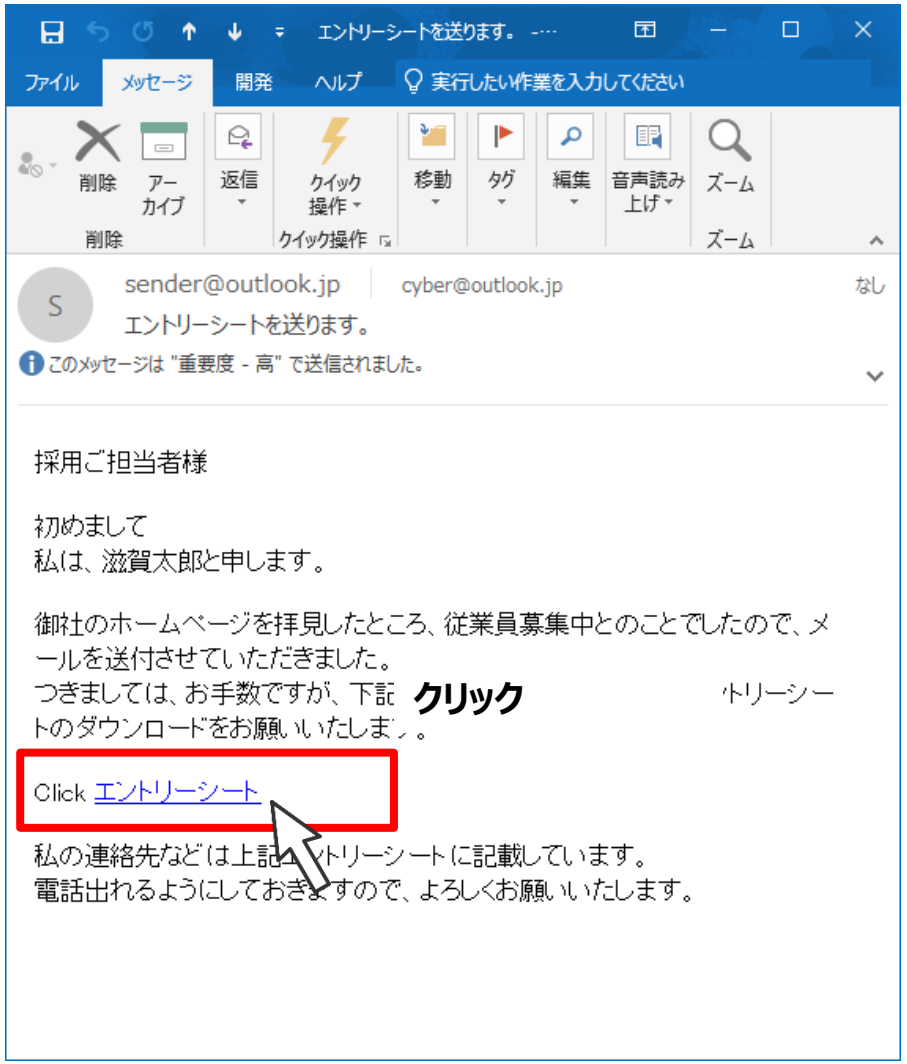
標的型メールの判別（本文中リンク）

1．次に、メールボックスの２番目のメールをクリックしてください。



上から２番目のメールをダブルクリックしてください。

標的型メールの判別（本文中リンク）



2．メール本文中にある「エントリーシート」をクリックしてください。

標的型メールの判別（本文中リンク）

3．インターネットに接続されWebサイトが表示されます。
（今回はダミーサイト）

Webサイトにアクセスした時点で、ウイルスファイルがダウンロードされます。

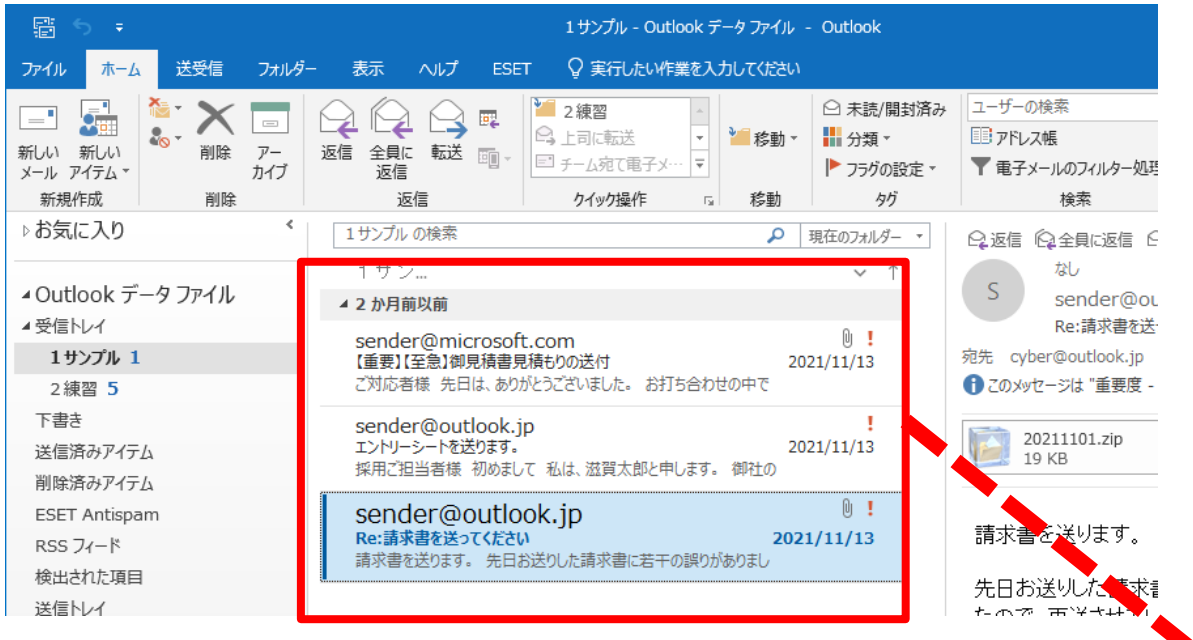
また、フィッシングサイトの場合もあります。

「×」ボタンで閉じてください。

メール本文中のリンク（URL）は、アクセスしないことが鉄則です。

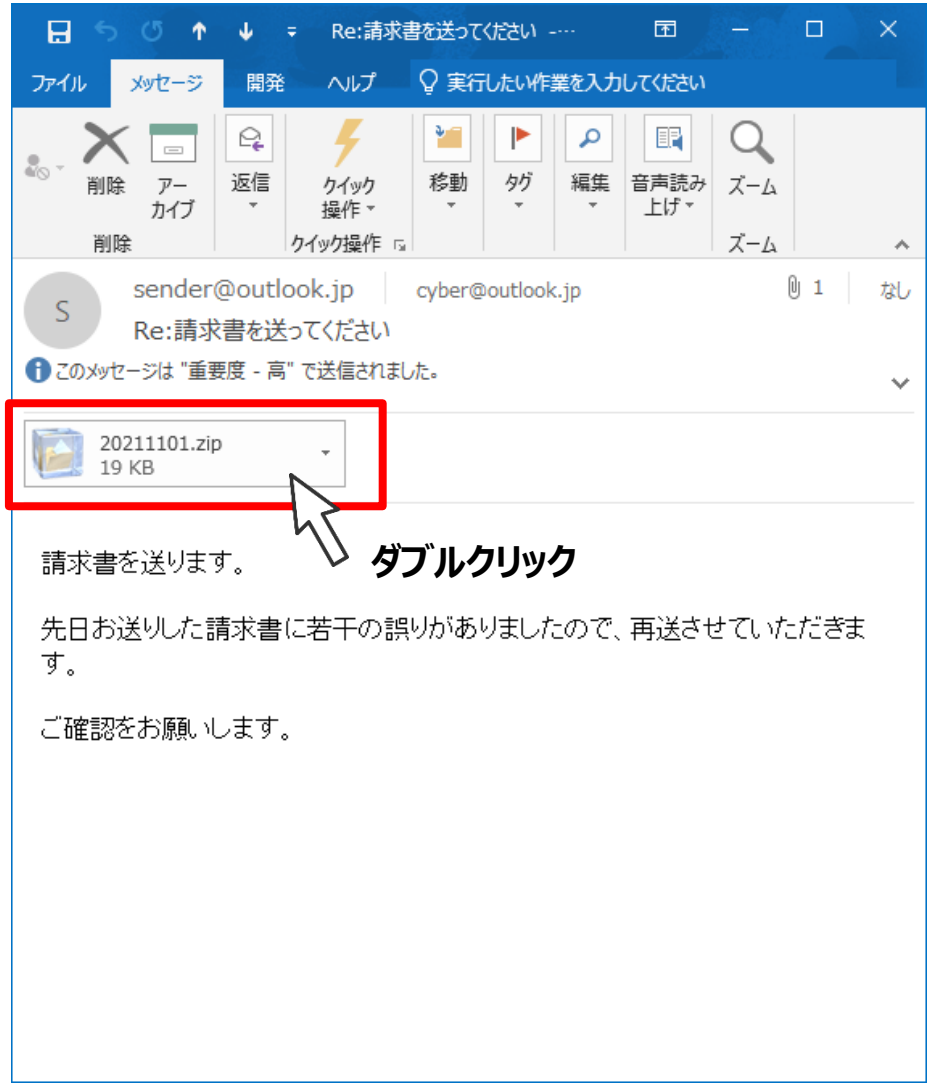
標的型メールの判別（ファイルレス攻撃）

1．最後に、メールボックスの３番目のメールをクリックしてください。

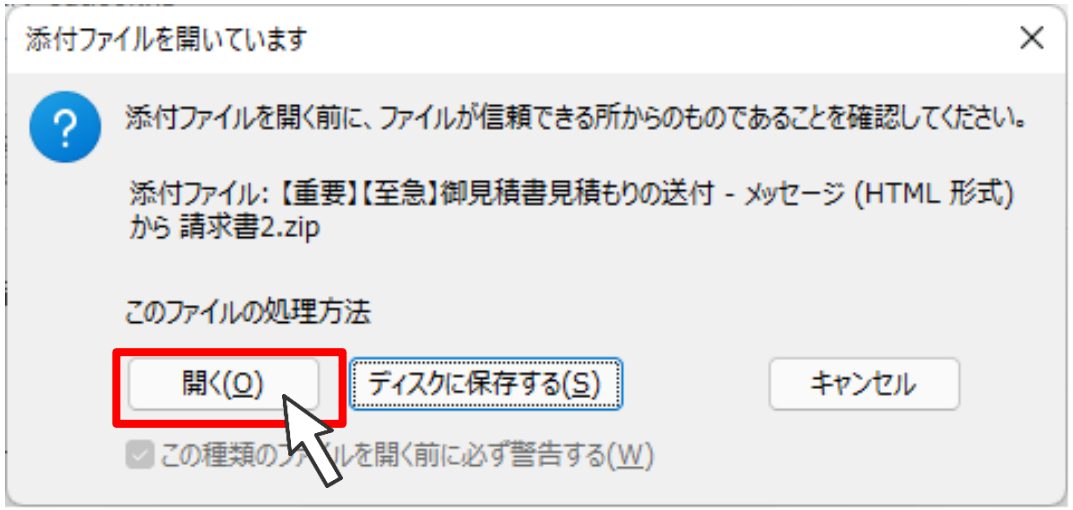


3番目のメールをクリックしてください。

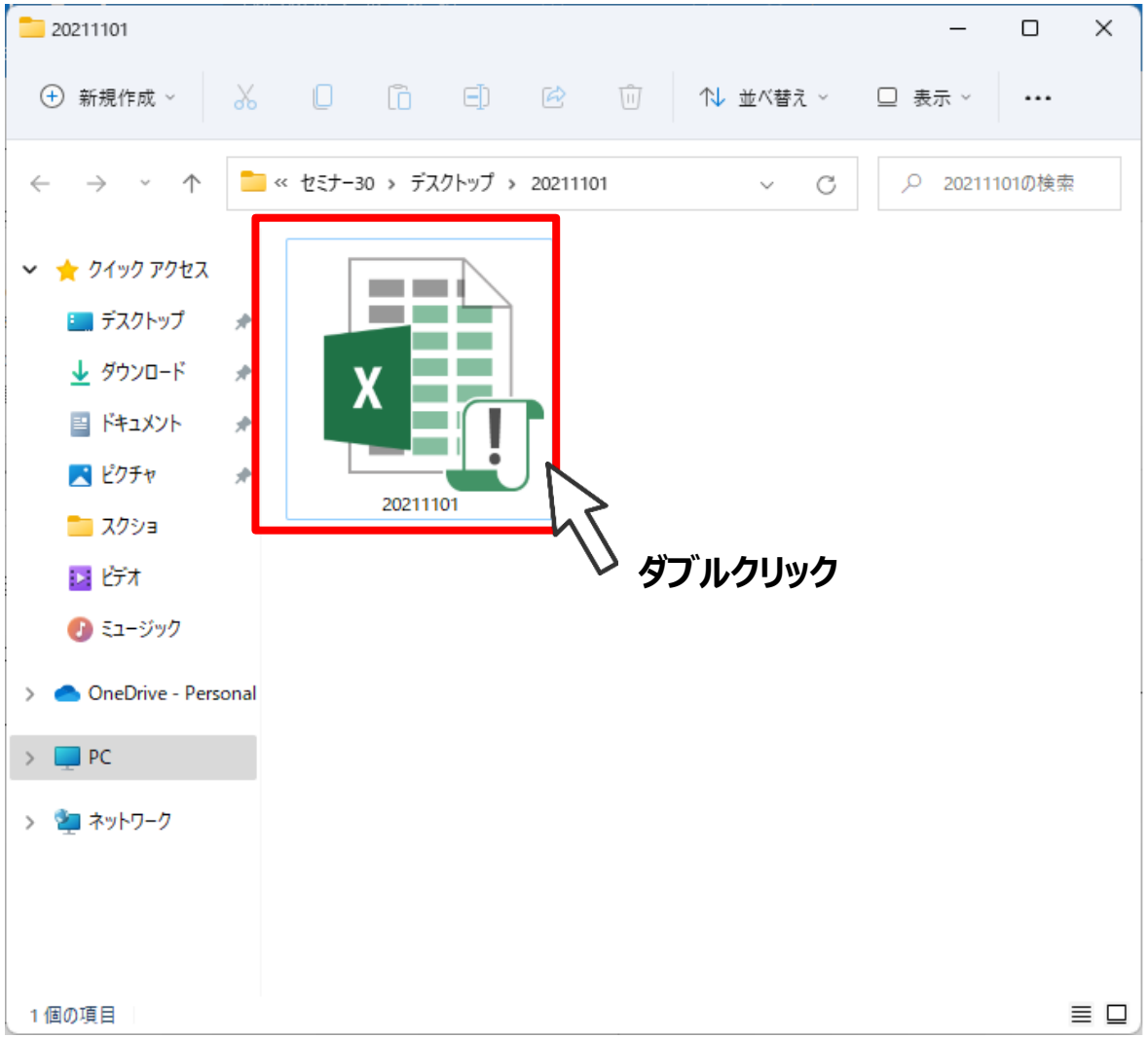
標的型メールの判別（ファイルレス攻撃）



2. 添付ファイルをダブルクリックしてください。
「添付ファイルを開いています」というメッセージが開きますので、
「開く」を押してください。
（デスクトップにファイルが保存されます。）

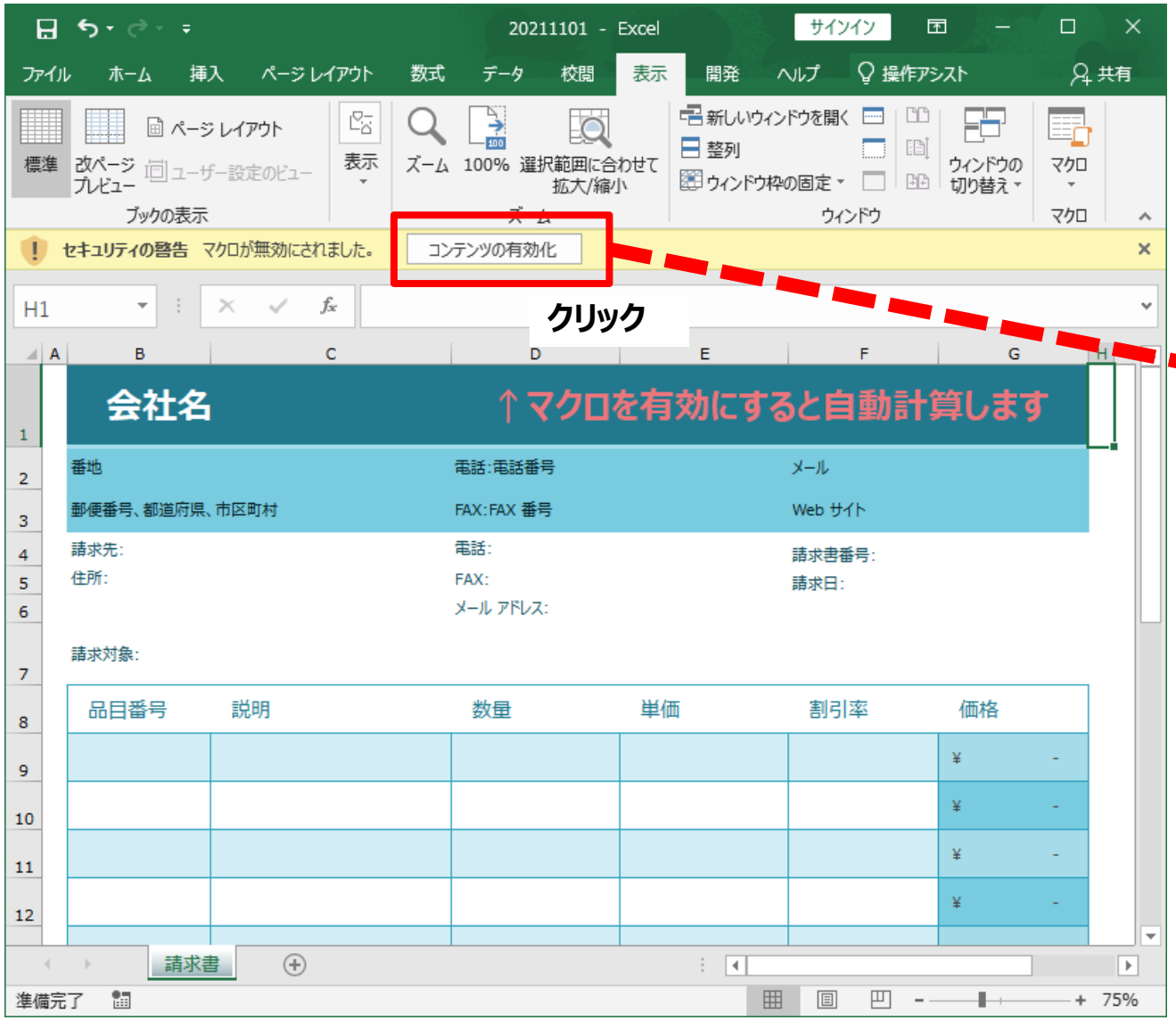


標的型メールの判別（ファイルレス攻撃）

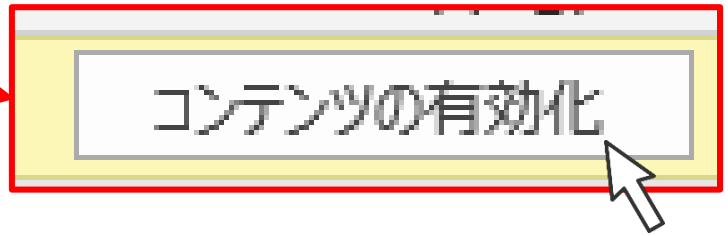


3. フォルダが開き、エクセルファイルが1つ表示されますのでダブルクリックして開いてください。

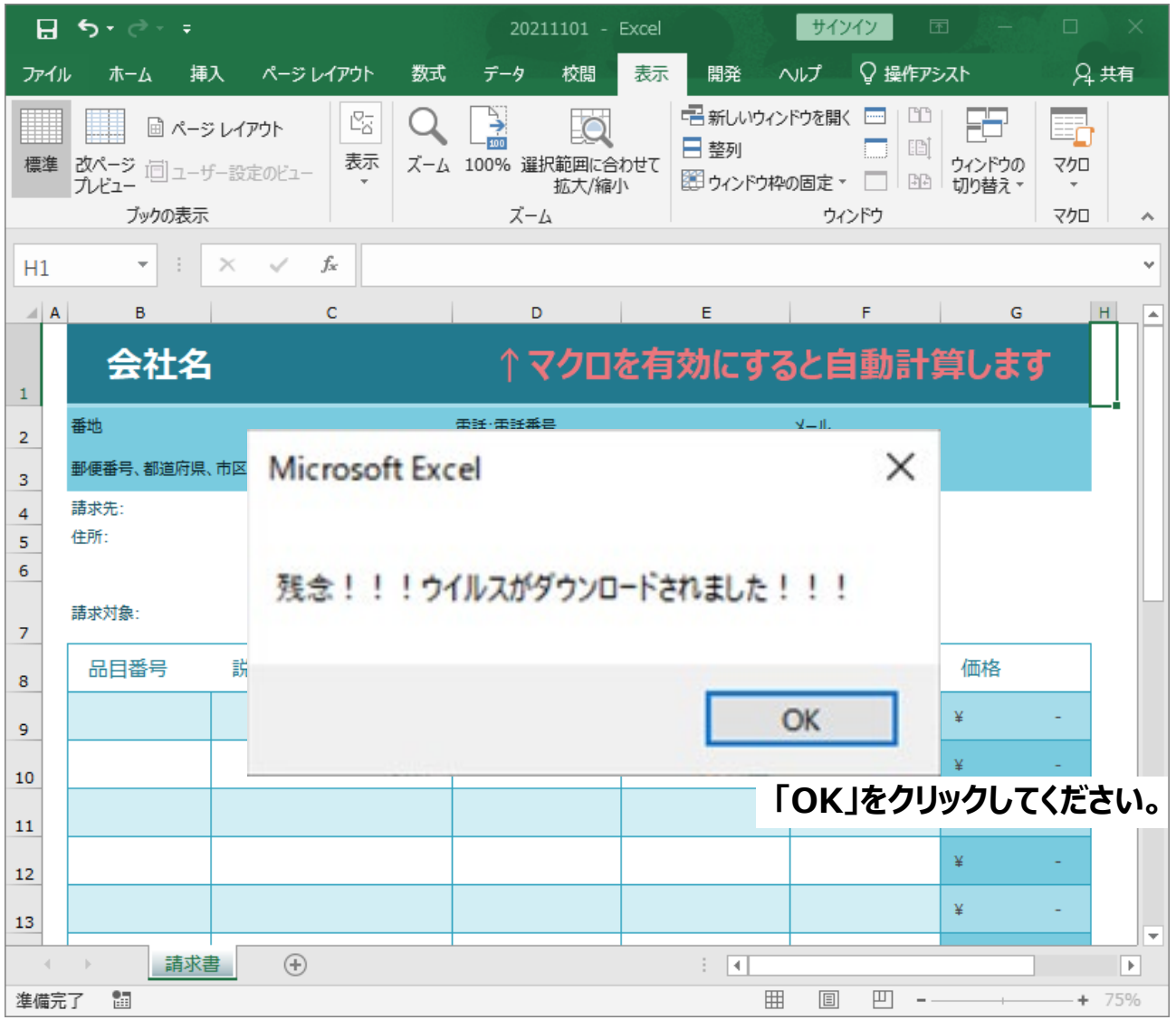
標的型メールの判別（ファイルレス攻撃）



4. 請求書のエクセルファイルが開きます。
さらに、「マクロを有効にすると自動計算します」と表示されているので、「コンテンツの有効化」ボタンを押してください。



標的型メールの判別（ファイルレス攻撃）

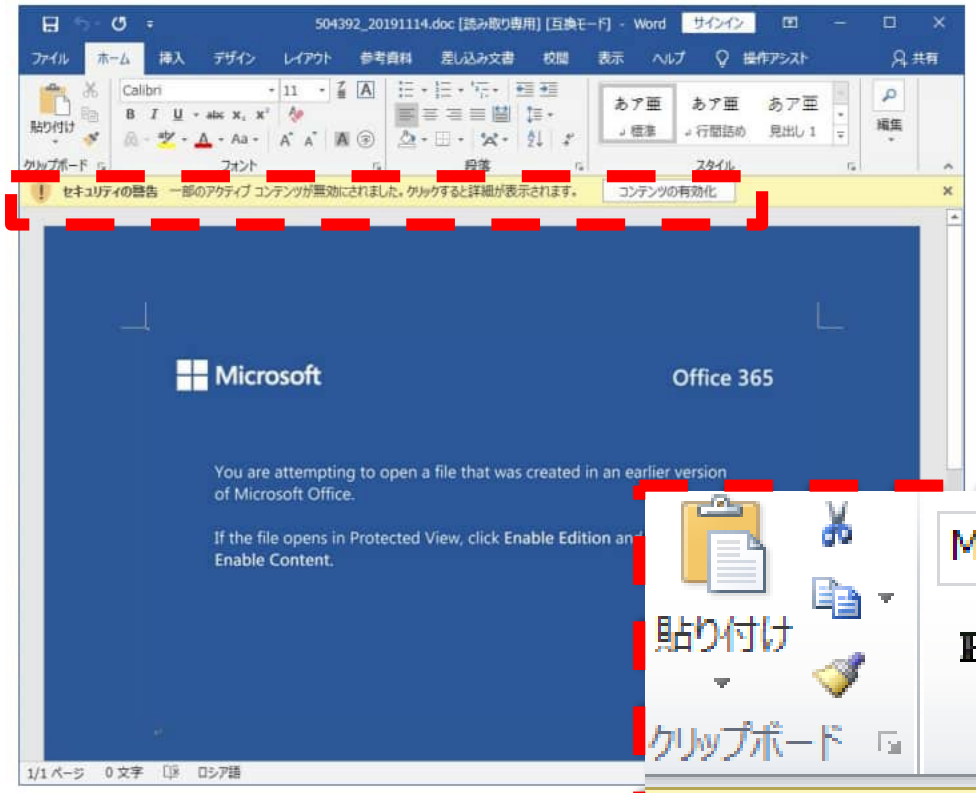


5. マクロプログラムが実行されました。
   マクロプログラムは、マイクロソフトのOfficeソフト用のプログラムです。
   インターネットからウイルスをダウンロードして感染させるというプログラムが確認されています。
   （通常、マクロは無効に設定されています。）

ファイルそのものは無害であるため「ファイルレス攻撃」と呼ばれています。

ファイルレス攻撃の代表的なウイルスに「Emotet」があります。

Emotetの仕組み

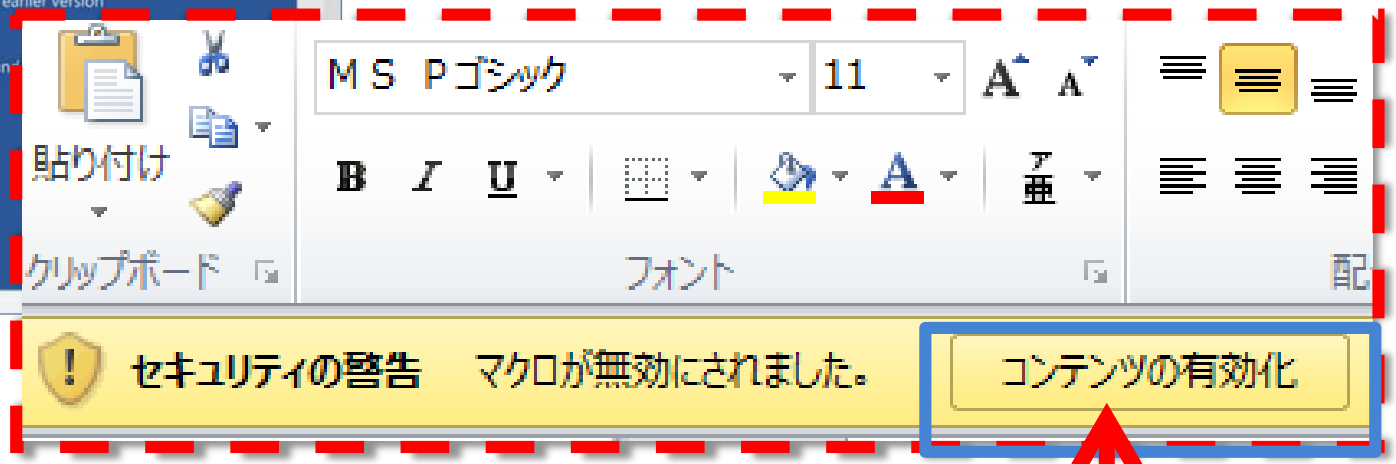


例：Wordの場合

Officeソフトに使われるマクロプログラムを有効にするには「コンテンツ」を有効にする必要があります。

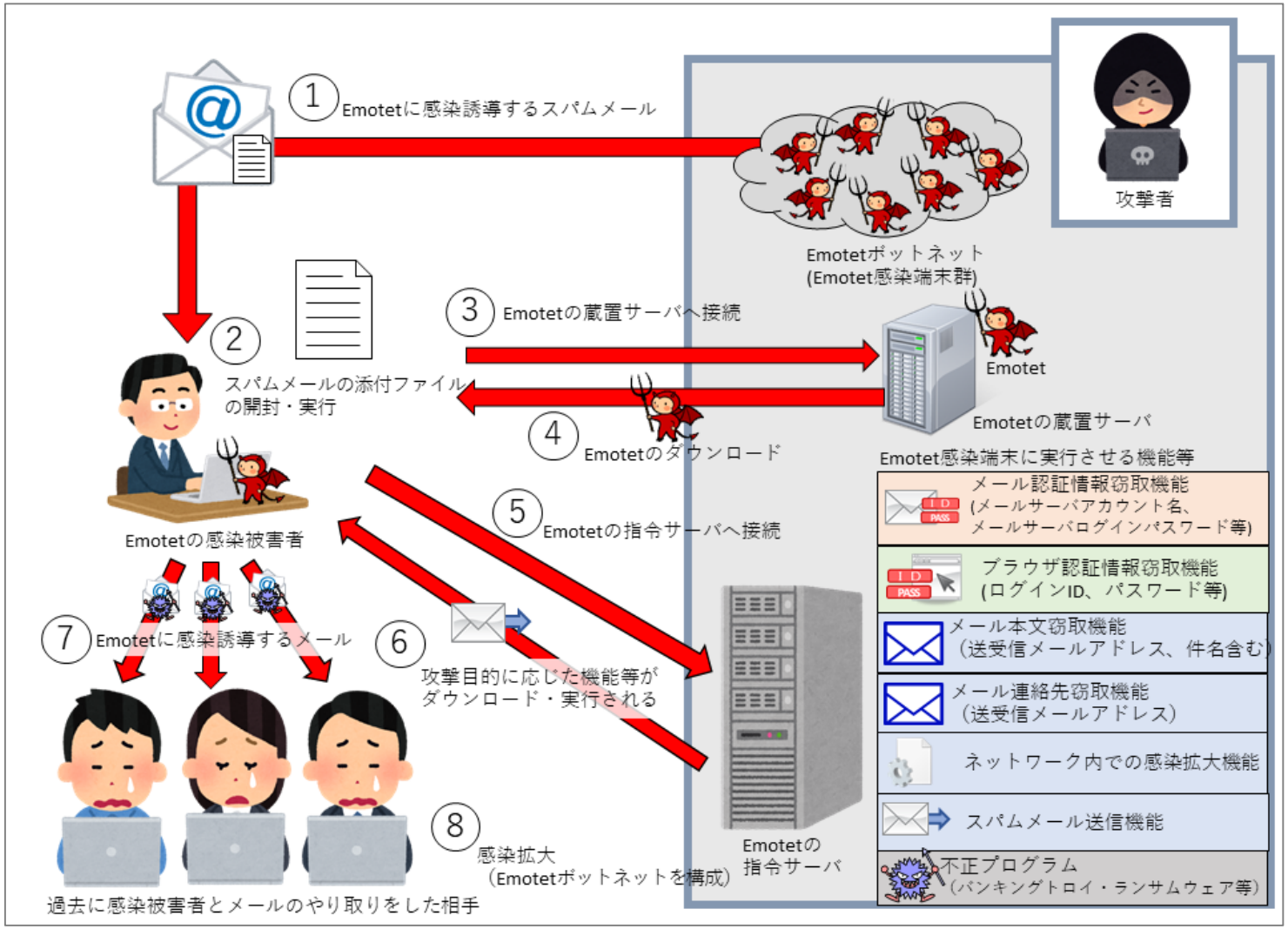
Emotetは、「コンテンツの有効化」ボタンを押すと、不正プログラムが実行され、外部サーバからウイルスをダウンロードする仕組みです。

ウイルスに感染すると情報を窃取され外部サーバに送信され、なりすましメールを送られるなどします。



クリックすると不正プログラムが実行（ダウンロード）される。

Emotetの仕組み



Emotetは2019年ころに確認され、活動と再開を繰り返しています。

2021年には、ユーロポールによってEmotetに利用されていたサーバが摘発されましたが、サーバや手口を変化させつつ活動を繰り返しています。

2022年２月ころ
日本国内で急速に拡大

2022年2月～4月
滋賀県内で多数のEmotetとみられる不審メールが確認された

2022年11月「信頼済みフォルダ」を利用した新たな手口が確認

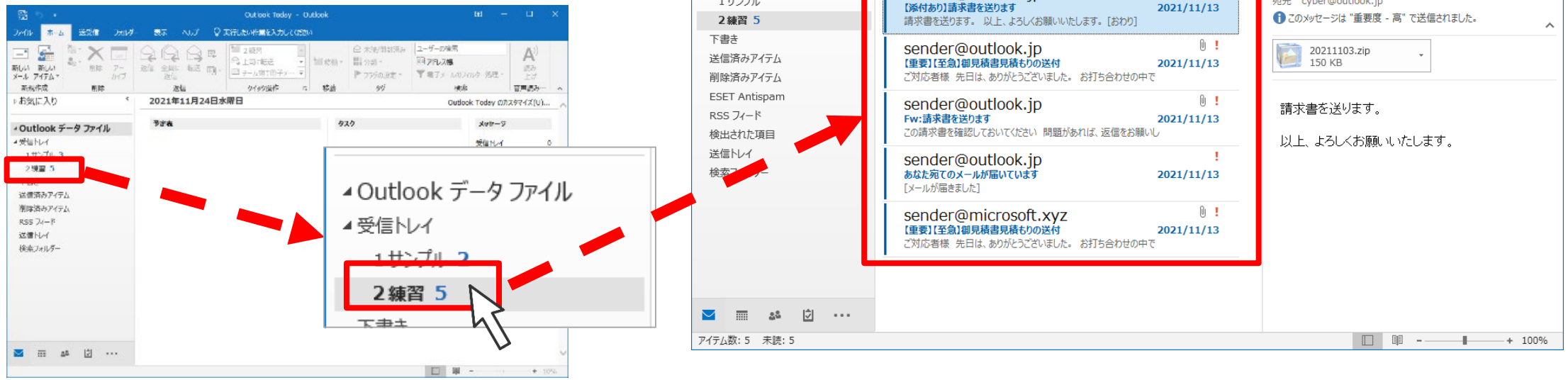
引用：警察庁「Emotetの解析結果について」 https://www.npa.go.jp/bureau/cyber/koho/detect/202012111.html

標的型メールの判別（総合）

1. これまでの標的型メールの判別の練習をしてみてください。
   受信トレイに「２練習」のフォルダをクリックしてください。

2. メールが複数ありますので、
   無害メールを探してください。

3. すべてのメールの添付ファイル
   を開いて確認してください。



標的型メール攻撃の対策

【ポイント】

- 送信者が信用できるか。
  送信元アドレスがフリーメールでないか。
- 添付ファイルを安易に開かない。
  開く場合は、ファイル形式の確認を。
- メール本文中のリンクをクリックしない。
- officeファイルのマクロにも注意。
  （Emotetに注意）

3　サイバーセキュリティ対策のポイント

- **経営者が考えるべきサイバーセキュリティ対策のポイントを説明します。**
- **セキュリティ対策基礎8項目を説明します。**

事業継続ができる体制を

- サイバー攻撃は完全に防ぐことが困難になっています。
- サプライチェーン上に被害が拡大するおそれがあります。

【対策のポイント】

攻撃を受けた場合でも被害を最小限にして、事業が継続できるように対策を考えておく必要があります。

防御
・アクセス権の強化
・暗号化
・分散管理
対処
・流出量の把握
・個人情報保護委員会への報告
・顧客への対応

サイバー攻撃の被害

情報漏えい

システム障害

脆弱性への対応
・セキュリティパッチの適用
・アップデート
バックアップの取得
バックアップから復旧手順の確認

損害発生・事業停止

- リスクマネジメント（分析・評価・対策）・・・リスクファイナンシング
- インシデントレスポンス（被害発生時の対応要領）
- 災害として対応（BCPに基づく）

事業継続ができる体制を

➢ 情報漏えいによるマイナスの影響を事前に予想する

情報技術（ＩＴ）の普及、活用により経営効率が向上した反面、ＩＴの普及以前に想定していなかった秘密情報や個人情報の漏えいによる高額賠償請求事例や金銭的損失を伴う事故が増えています。

企業が被る主な不利益

金銭的損失	顧客の喪失	業務の喪失	従業員への影響
• 調査費用 • 損害賠償 • 業務停滞	• 信用失墜 • 取引解除	• サービス、システムの停止 • 営業機会の喪失	• 意欲の低下 • 企業イメージダウン

インシデントハンドリング（インシデント発生時の対応要領）

①	**検知 連絡受付**	・インシデントの認知 ・責任者への報告	・従業員からの連絡 ・外部からの情報提供　等 ・情報源の正確性の確認
②	**トリアージ**	・事実確認 ・インシデント該当性判断 ・対応の優先順位つけ	・インシデントと判断した場合、被害状況と重要度に基づいて対応の優先順位を決定
③	**インシデント レスポンス**	・対応方針の検討 ・証拠保全、調査 ・被害原因の除去	・事業継続できる状態か ・警察への通報、関係者への連絡 ・原因解明のための措置
④	**事後対応**	・組織内外に報告、公表 ・対策の検証、改善	・公表の可否を検討 ・再発防止対策の検討、実施

通報・連絡先

- **保守業者、IT業者**
  対応、復旧、証拠保全の要請
- **警察**
  サイバー攻撃、またはそのおそれがある場合
- **個人情報保護委員会**
  個人情報が流出した場合
  （個人情報保護法による義務）

参照：JPCERT/CC　インシデントハンドリングマニュアル
https://www.jpcert.or.jp/csirt_material/files/manual_ver1.0_20211130.pdf

情報セキュリティ対策ガイドライン

◆経営者が認識すべき「3原則」

1. 情報セキュリティ対策は経営者のリーダーシップで進める。

2. 委託先の情報セキュリティ対策まで考慮する。

3. 関係者とは常に情報セキュリティに関するコミュニケーションをとる。

引用：ＩＰＡ「中小企業の情報セキュリティ対策ガイドライン第３.1版」
https://www.ipa.go.jp/security/guide/sme/about.html

情報セキュリティ対策の基礎８項目

情報セキュリティハンドブック（NISC）に紹介されている「情報セキュリティ対策の基礎8項目」をご紹介します。

1	OSやソフトウェアは常に最新にする	IT機器にはセキュリティホールが日々見つかっていますので、メーカーが提供している修正用アップデートを常に適用して、攻撃の糸口となる穴を塞ぎます。
2	ウイルス対策ソフトの導入	マルウェア（ウイルス）も日々進化しています、攻撃者の新たな手口に対抗するために、常に更新し続ける必要があります。
3	パスワードを強化する	攻撃者は、パスワードを推測して不正アクセスを行います。推測しにくいパスワードを設定するとともに、使い回さないことが重要です。
4	共有設定を見直す	ネットワーク上の共有ストレージを利用している場合、うっかり誰でも見られる状態にしていると情報が盗まれてしまいます。共有設定を確認することで情報を守ります。
5	脅威や攻撃の手口を知る	攻撃者は、常に新たな攻撃手段を開発します。攻撃の手口を知ることで回避できる攻撃があるため、情報収集が重要です。
6	常にバックアップをとる	正常なデータを複製保存しておくことで、仮に攻撃を受けて重要なファイルを失ってしまっても、復元することにより被害を軽減します。
7	人間にもセキュリティホールがあることを知る	攻撃者は、人間の錯誤、失敗、思い込み、油断等心の隙をついた攻撃を行いますので、人間のセキュリティホールも念頭に入れることが必要です。
8	困ったら各種相談窓口にすぐに相談する	攻撃を受けた場合の対応を検討しておき、相談窓口をあらかじめ確認しておくことが重要です。

内閣サイバーセキュリティセンター「（旧）小さな中小企業とNPO向け情報セキュリティハンドブック」「（新）インターネットの安心・安全ハンドブック[中小組織向け抜粋版]
https://security-portal.nisc.go.jp/guidance/handbook.html

警察にご連絡をお願いします。

- ランサムウェアに感染した。
- サーバに不正アクセスされた。
- 情報が流出した。
- DDoS攻撃を受けている。
- なりすましメールが送信されている。
- Webサイトが改ざんされた。

など

サイバー攻撃を受けた場合は、警察にご連絡をお願いします。
滋賀県警察本部サイバー犯罪対策課077-522-1231（代表）

【ポイント】

- **ネットワークを切断してください。**
  内部感染の拡大防止、外部への情報流出防止が重要です。
  → **LANケーブル･･･端末から外してください。**
  → **Wi-Fi（無線）･･･ネットワークを切断してくだい。**
- **電源は切らないでください。**
  → **メモリ上からデータが消えてしまい、調査ができなくなります。**
  メモリには、外部への通信履歴が残っていることがあります。
  再起動もしないでください。
- **システム担当者、または責任者、管理者に連絡してください。**

※サイバー攻撃の種類によって対処方法は異なります。

出張セミナー随時実施しています。
詳しくは、お問い合わせください。

終了

ご清聴ありがとうございました。

公式X（旧Twitter）@shiga_cyber

公式Webサイト

滋賀県警察　サイバー犯罪対策課077-522-1231（代表）

https://www.pref.shiga.lg.jp/police/seikatu/304409/index.html