社外秘

第7期システム移行しました！！

公社における情報システム使用に関する周知事項(令和6年度 その２)

企画総務課システム担当　広瀬

本動画の目的

①業務上の誤った機器操作などによるご自身や組織への不利益が
　生じないよう、ＩＴリテラシー向上に役立つ情報をお伝えします

②昨今ニュースなどでもよく耳にするようになった「サイバー攻撃」
　に関する知識を、公社のＩＴ環境も交えてお伝えします

③この動画は公社情報セキュリティ対策要綱第３条、並びに公社情報
　セキュリティ規定第６条に定める職員の教育等に寄与することを目
　的としています

社外秘

本動画でよく使う用語

第7期(公社)システム

第ｎ期システムとは公社のＩＴ機器リース入替のサイクルです。
５年度周期で入替を実施しており、今年度は第7期の1年目にあたります。

職員用端末(PC)、共用端末(PC)

皆さんの自席に置かれるPCを職員用端末、誰でも使えるPCを共用端末とします。
※上記以外のPCは特定端末として、本研修内容の対象外とします

サイバー攻撃

本動画ではインターネットを悪用して他者に損害を生じさせる行為とします。
※上記より広義のサイバー攻撃は本動画内容の対象外とします

本動画の流れ

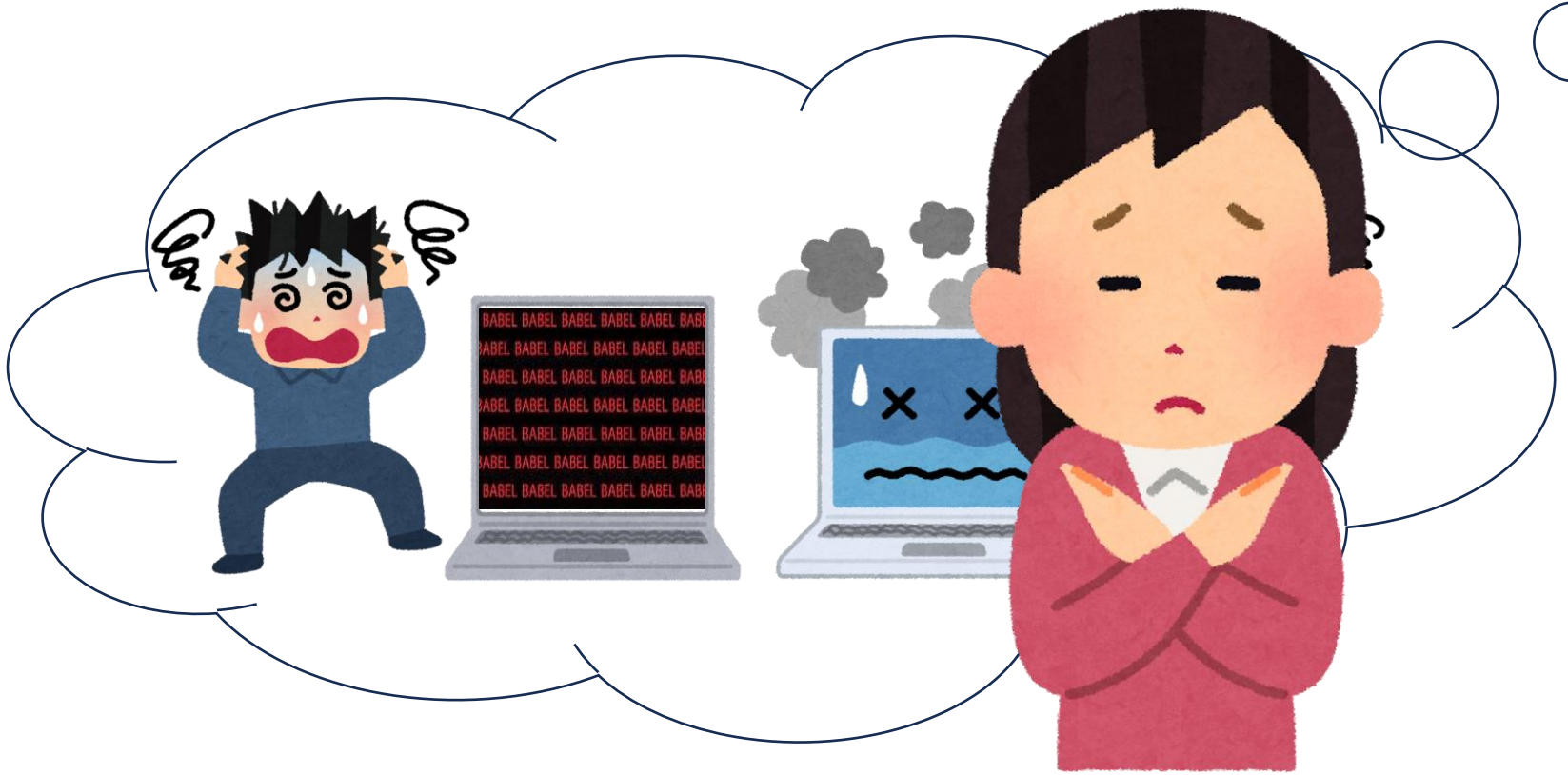
１　サイバー攻撃とは何か

２　最近のサイバー攻撃と、その手口

３　サイバー攻撃に備えましょう

最後に

1　サイバー攻撃とは何か



図のようなサイバー攻撃は、昨今主流ではありません。

最近のサイバー攻撃のトレンドを一言で例えるならば「データ泥棒」が最も実態に近いでしょう。

1　サイバー攻撃とは何か

なぜサイバー攻撃に備えるのか

現代社会において、サイバー攻撃に備えることは標準的な防犯思想といえます。

店舗に泥棒が入ったら…

- ●お金を盗まれる
- ●物を壊される
- ●鍵や社員証などを盗まれる
- ●名簿や連絡先を盗まれる
- ●設計図やレシピを盗まれる

ネットワークに侵入されたら…

- ●ネットバンキング情報が知られる
- ●PCなどが正常に動かなくなる
- ●ID・パスワード情報が流出する
- ●個人情報データが流出する
- ●社外秘データが流出する

金銭的被害

社会的信用の失墜

社外秘

1　サイバー攻撃とは何か

サイバー攻撃の目的とは？

サイバー攻撃の目的は、主に次の三つが挙げられます。

① 金銭の詐取

犯罪者間で分業化も進んでいる(ビジネス化の過熱傾向)

② 機密情報の窃取

- 個人情報
- パスワードや金融関連情報
- 市場競争力を有する情報

情報がダークウェブで売買される

③ 個人(組織)的信条の表明・行使

“ハクティビズム”とも呼ばれ、「アノニマス」「ウィキリークス」などが有名

社外秘

2　最近のサイバー攻撃と、その手口

IPA発表「情報セキュリティ10大脅威 2024（個人編）」

「個人」向け脅威（五十音順）	初選出年	10大脅威での取り扱い（2016年以降）
インターネット上のサービスからの個人情報の窃取	2016年	5年連続8回目
インターネット上のサービスへの不正ログイン	2016年	9年連続9回目
クレジットカード情報の不正利用	2016年	9年連続9回目
スマホ決済の不正利用	2020年	5年連続5回目
偽警告によるインターネット詐欺	2020年	5年連続5回目
ネット上の誹謗・中傷・デマ	2016年	9年連続9回目
フィッシングによる個人情報等の詐取	2019年	6年連続6回目
不正アプリによるスマートフォン利用者への被害	2016年	9年連続9回目
メールやSMS等を使った脅迫・詐欺の手口による金銭要求	2019年	6年連続6回目
ワンクリック請求等の不当請求による金銭被害	2016年	2年連続4回目

社外秘

出展：独立行政法人 情報処理推進機構(IPA)ホームページより　https://www.ipa.go.jp/security/10threats/10threats2024.html

「個人」向け脅威（五十音順）	初選出年	10大脅威での取り扱い（2016年以降）
インターネット上のサービスからの個人情報の窃取	2016年	5年連続8回目
インターネット上のサービスへの不正ログイン	2016年	9年連続9回目
クレジットカード情報の不正利用	2016年	9年連続9回目
スマホ決済の不正利用	2020年	5年連続5回目
偽警告によるインターネット詐欺	2020年	5年連続5回目
ネット上の誹謗・中傷・デマ	2016年	9年連続9回目
フィッシングによる個人情報等の詐取	2019年	6年連続6回目
不正アプリによるスマートフォン利用者への被害	2016年	9年連続9回目
メールやSMS等を使った脅迫・詐欺の手口による金銭要求	2019年	6年連続6回目
ワンクリック請求等の不当請求による金銭被害	2016年	2年連続4回目

社外秘

出展：独立行政法人 情報処理推進機構(IPA)ホームページより　https://www.ipa.go.jp/security/10threats/10threats2024.html

2　最近のサイバー攻撃と、その手口

IPA

IPA発表「情報セキュリティ10大脅威 2024（組織編）」

順位	「組織」向け脅威	初選出年	10大脅威での取り扱い（2016年以降）
1	ランサムウェアによる被害	2016年	9年連続9回目
2	サプライチェーンの弱点を悪用した攻撃	2019年	6年連続6回目
3	内部不正による情報漏えい等の被害	2016年	9年連続9回目
4	標的型攻撃による機密情報の窃取	2016年	9年連続9回目
5	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	2022年	3年連続3回目
6	不注意による情報漏えい等の被害	2016年	6年連続7回目
7	脆弱性対策情報の公開に伴う悪用増加	2016年	4年連続7回目
8	ビジネスメール詐欺による金銭被害	2018年	7年連続7回目
9	テレワーク等のニューノーマルな働き方を狙った攻撃	2021年	4年連続4回目
10	犯罪のビジネス化（アンダーグラウンドサービス）	2017年	2年連続4回目

社外秘

出展：独立行政法人 情報処理推進機構(IPA)ホームページより　https://www.ipa.go.jp/security/10threats/10threats2024.html

順位	「組織」向け脅威	初選出年	10大脅威での取り扱い（2016年以降）
1	ランサムウェアによる被害	2016年	9年連続9回目
2	サプライチェーンの弱点を悪用した攻撃	2019年	6年連続6回目
3	内部不正による情報漏えい等の被害	2016年	9年連続9回目
4	標的型攻撃による機密情報の窃取	2016年	9年連続9回目
5	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	2022年	3年連続3回目
6	不注意による情報漏えい等の被害	2016年	6年連続7回目
7	脆弱性対策情報の公開に伴う悪用増加	2016年	4年連続7回目
8	ビジネスメール詐欺による金銭被害	2018年	7年連続7回目
9	テレワーク等のニューノーマルな働き方を狙った攻撃	2021年	4年連続4回目
10	犯罪のビジネス化（アンダーグラウンドサービス）	2017年	2年連続4回目

IPA

社外秘

出展：独立行政法人 情報処理推進機構(IPA)ホームページより　https://www.ipa.go.jp/security/10threats/10threats2024.html

2　最近のサイバー攻撃と、その手口

キングオブサイバー攻撃「ランサムウェア」

【名前の由来】

身代金(ransom)とマルウェア(malware)を合わせた造語です

※マルウェアとは不正なソフトウェアの総称です

【ランサムウェアの特徴】

〇感染したPC・ネットワーク内のファイルを暗号化してしまう

〇暗号化と並行してファイルのデータを攻撃者側のネットワークへ持ち出す

〇暗号化したファイルの復号・返還と引き換えに金銭を要求する(二重脅迫型)

社外秘

被害の一例　（すごく有名なもの）

2020年6月

　愛知県の大手自動車メーカー関連工場が感染。１日システムダウンした結果、国内外９工場に影響し、計13,000台の生産遅延につながった。

2020年11月

　大手ゲーム開発会社が感染し、顧客情報含めた機密情報が約1TB漏洩した。

2021年10月

　徳島県内の公立病院が感染し、電子カルテ等情報をすべて喪失。2ヶ月にわたり新規患者の受け入れができない状況が続いた。

　既存患者は災害対策マニュアルに基づいて診療を続行した。

2023年6月

　社会保険労務士事務所向けサービス提供ベンダーが感染し、サービスが約1ヶ月停止。最大で750万人弱の個人情報漏洩のおそれが報告された。

2023年7月

　名古屋港のコンテナターミナルが感染。コンテナ搬出入作業が丸一日停止するも、オフラインのバックアップから早期復旧を果たした。

社外秘

ランサムウェア被害の一例　（すごく有名なもの）

2020年6月

　愛知県の大手自動車メーカー関連工場が感染。１日システムダウンした結果、国内外９工場に影響し、計13,000台の生産遅延につながった。

2020年11月

　大手ゲーム開発会社が感染し、顧客情報含めた機密情報が約1TB漏洩した。

2021年10月

　徳島県内の公立病院が感染し、電子カルテ等情報をすべて喪失。2ヶ月にわたり新規患者の受け入れができない状況が続いた。

　既存患者は災害対策マニュアルに基づいて診療を続行した。

ＢＣＰ（Business Continuity Plan、事業継続計画）

　災害などの緊急事態が発生したときに、組織が損害を最小限に抑え、事業の継続や復旧を図るための計画。

　緊急事態について既存の災害対策マニュアル等が発生時の初動特化であるのに対し、本来業務を主眼に置いて組織に与える影響を包括的に評価するのが特徴。

　日本ではコロナ禍でのオフィス人員の急減に対応する必要性から注目が高まった。

社外秘

2024年の被害事例　（すごく有名なもの）

出版・エンターテイメントグループ企業の被害

2024年6月9日、国内大手出版・エンターテイメントグループ企業の動画投稿サイトなどをはじめとしたWebサイトが閲覧不可となる被害が発生。

当初はDDos攻撃(大量アクセス)による一時的なサーバダウンとされていたが、後にランサムウェアによる攻撃と判明。

犯行グループから犯行声明とともに身代金要求をされたが決裂した模様で、窃取されたデータが7月1日以降ダークウェブに流出したことが確認された。

情報処理・機器サービス企業の被害

2024年5月26日、京都に本社がある国内大手情報処理・機器サービス企業がランサムウェアに感染し、保有データを窃取される被害が発生。

当該企業は主に関西圏を中心として多くの地方自治体・公共団体の事業受託をしており、その業務に関する個人情報の流出が懸念されていた。

当初は「情報漏洩は確認されていない」としていたものの、その後6月18日にダークウェブに個人情報を含むデータの流出を確認した旨を公表した。

2　最近のサイバー攻撃と、その手口

その他のサイバー攻撃の手法

〇サプライチェーン攻撃

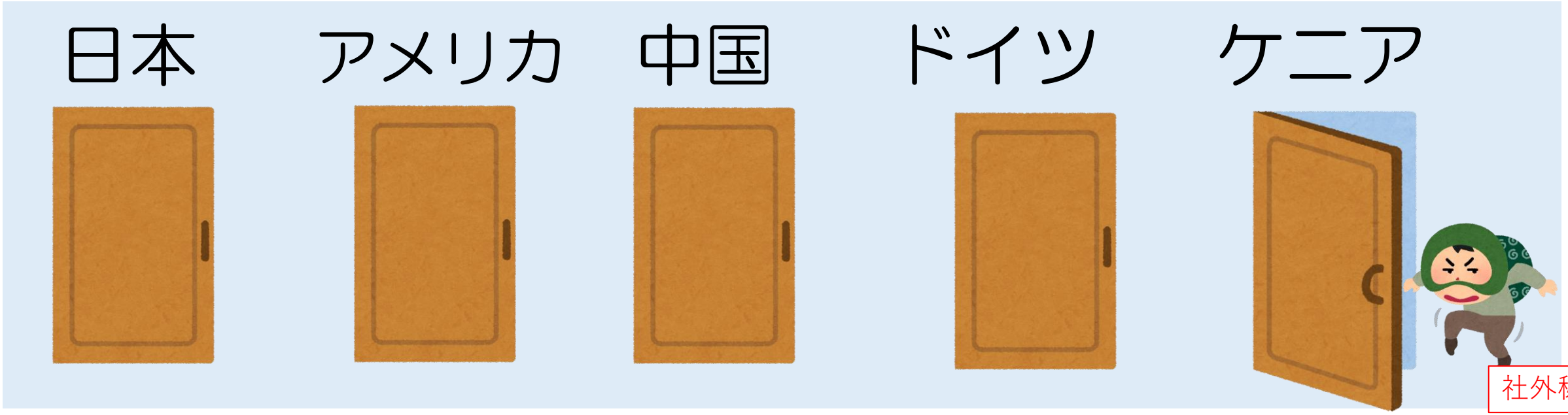
　主に製造業や小売業において「原料～生産(加工)～物流～販売～顧客」と連なるネットワークについて、比較的脆弱な箇所からネットワーク全体への侵入を試みる攻撃手法です。

2　最近のサイバー攻撃と、その手口

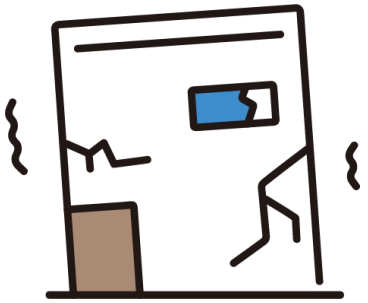
その他のサイバー攻撃の手法

〇サプライチェーン攻撃

　主に製造業や小売業において「原料～生産(加工)～物流～販売～顧客」と連なるネットワークについて、比較的脆弱な箇所からネットワーク全体への侵入を試みる攻撃手法です。



2　最近のサイバー攻撃と、その手口



その他のサイバー攻撃の手法

○標的型攻撃

　標的となる個人・組織を絞り込み、攻撃の成功率を上げるために様々な工夫をこらす攻撃手法です。

下調べ

公式WEBサイト
- 取扱製品（サービス）
- 主要取引先
- 営業拠点
- 組織図

ダークウェブ
- パスワード
- IDなどの認証情報
- 人員や役職の情報
- メール情報

攻撃準備

アドレスの収集
メール情報の解析
↓
標的（部署・個人）の選定
↓
偽装送信元の選定
↓
メール文の作成
マルウェアの用意

攻撃

巧みに実在の取引を装って金銭を詐取するビジネスメール詐欺（BEC）を仕掛けることも

題名：【緊急】（実在案件）につきまして
送信：〇〇商事　△△（←実在の人物）
宛先：第一営業部▲▲（←実際の担当者）

本文

株式会社□□ 第一営業部 営業二課
▲▲様

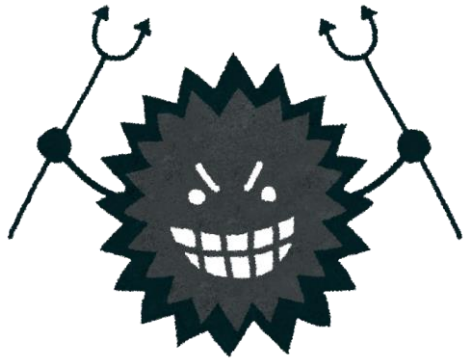
いつもお世話になっております。
〇〇商事の△△です。

表題の件ですが、原材料の輸入について現地から緊急情報が入りましたので善後策を協議させてください。
現地情報は以下のURLでご確認ください。
https://www.akui.higai.com/malware/dl/

△△の定型署名

社外秘

2　最近のサイバー攻撃と、その手口



ランサムウェアなどのマルウェアに感染する経路

　ランサムウェアなどのマルウェアに感染してしまう経路としては、次のような手口が知られています。

○PC・ネットワークの入口を発見され、突破されてしまう

○感染した他のネットワークから流入してくる

○ランサムウェアなどの媒体となるファイルを実行してしまう

公社は三番目の経路に注意しましょう

社外秘

2　最近のサイバー攻撃と、その手口

不正なファイル実行にご用心！

公社のネットワーク環境においては、マルウェアに感染してしまう最も大きなリスクは不正なファイルを実行してしまうことです。
不正なファイルを実行してしまう状況は次のように考えられます。

○メールに添付されていたファイルが不正なファイルだった

○Webサイトからダウンロードしたら不正なファイルだった

ファイルのマクロを有効化したらマルウェアがダウンロード！

なんてことがあるかも…

不審なメールやWebサイトにはご用心ください

社外秘

ランサムウェア攻撃の初期アクセス経路

出典：ランサムウェア攻撃から企業を守る
侵入経路別の対策方法(ソフトバンク社)

ランサムウェア攻撃には大きく分けて５つの経路が存在する

ランサムウェアを用いた攻撃を行う人物またはグループは、さまざまな手口を使って侵入を試みます。 そのため、それぞれのアクセス経路に応じた対策が重要になります。

Case1
メール経由
メールに添付されたURLリンクやファイルを実行すると感染する。

詳しくは９ページ

Case2
脆弱性と認証
さまざまな機器、ソフトウェアの脆弱性に対する攻撃や認証を突破して侵入。

詳しくは11ページ

Case3
先行マルウェア
予め別の経路から感染していた先行マルウェアがランサムウェア攻撃者の侵入経路を作るケース。Emotetなど。

詳しくは13ページ

Case4
MSP,サプライヤ
MSPやサプライヤを介して侵入する。

詳しくは15ページ

Case5
内通者
攻撃者が組織内の関係者に買収を持ち掛け、情報提供または内通者自身がマルウェアを実行することで侵入。

詳しくは17ページ

社外秘

社外秘

出典：ランサムウェア攻撃から企業を守る
侵入経路別の対策方法(ソフトバンク社)

Case1:メール経由による侵入

悪意あるメールから感染するもっともポピュラーな手法

信頼できないメールから感染するポピュラーな手法です。

これらのメール本文に記載されたURLをクリックしたり、添付されたファイルを実行することで、マルウェアに感染したり、攻撃者の侵入を許してしまうこととなります。
直接的な感染の原因となることが多いですが、この行動が引き金となって、さらなるマルウェア感染や情報流出などの被害が発生するケースもあります。

・メールフィルタリングを使用して悪意のあるメールをブロックする。
・従業員教育を実施し、添付ファイルやリンクを開く前に確認する習慣を身につける。
・文書ファイル（Office系やPDFなど）を扱うソフトウェアを常に最新にする。
・マクロブロックなどの機能を用いる。
・EDRなどのエンドポイント対策を講じる。

社外秘

社外秘

2　最近のサイバー攻撃と、その手口

不正なファイル実行にご用心！

公社のネットワーク環境においては、マルウェアに感染してしまう最大のリスクは不正なファイルを実行してしまうことです。

不正なファイルを実行してしまう

怪しいマクロは敵だ！

（　　）ダウンロードしたら不正なファイルだった

ファイルのマクロを有効化したらマルウェアがダウンロード！

なんてことがあるかも…

不審なメールやWebサイトにはご用心ください

社外秘

2　最近のサイバー攻撃と、その手口

侮れない「サポート詐欺」の被害

　一般的なWebサイトを閲覧中、急に「ウイルスに感染した」旨の画面が表示され、それに加えてPCの操作が著しく制限されます。

　画面上にはMicrosoftなどのメーカーを称したサポートセンターの電話番号もあわせて表示され、事態の改善につながるように見えます。

被害報告が急増中！

①サポート費用を請求されます

　多くの場合、Amazonギフトカードなどのプリペイド式を指定してくるようです

②パソコンの操作を乗っ取られます

　修復のため、などと称してリモートアクセスアプリをダウンロードさせるようです

社外秘


サポート
再起動または使用しないでください あなたのコンピュータ.
コンピューターが無効になっています。私に電話してください。
アクセスはこれのブロックセキュリティの理由です コンピュータ。
すぐにご連絡ください。 技術者が問題の解決をお手伝いします.
お使いのコンピュータは、トロイの木馬スパイウェアに感染していること
WindowsDefenderセキュリティセンター
アプリ: Ads.fiancetrack(2).dll
検出された脅威：トロイの木馬スパイウェア
このPCへのアクセスはセキュリティ上の理由でブロックされています。
Windowsサポートに連絡する: (050) 50 -1 3 (通話料無料)
マイクロソフト
拒否
許可する
止されます。登録.
Microsoftサポートに連絡する: (050) 5050-1173 (通話料無料)

社外秘

サポート詐欺による被害の一例

2023年7月

　鹿児島県日置市の市立校でマルウェアをインストールされ、市内20校の校務システムが一時停止

2024年2月

　山梨県笛吹市商工会でインターネットバンキングを不正操作され約1000万円の被害(個人情報にもアクセス可能なPCだったとのこと)

2024年3月

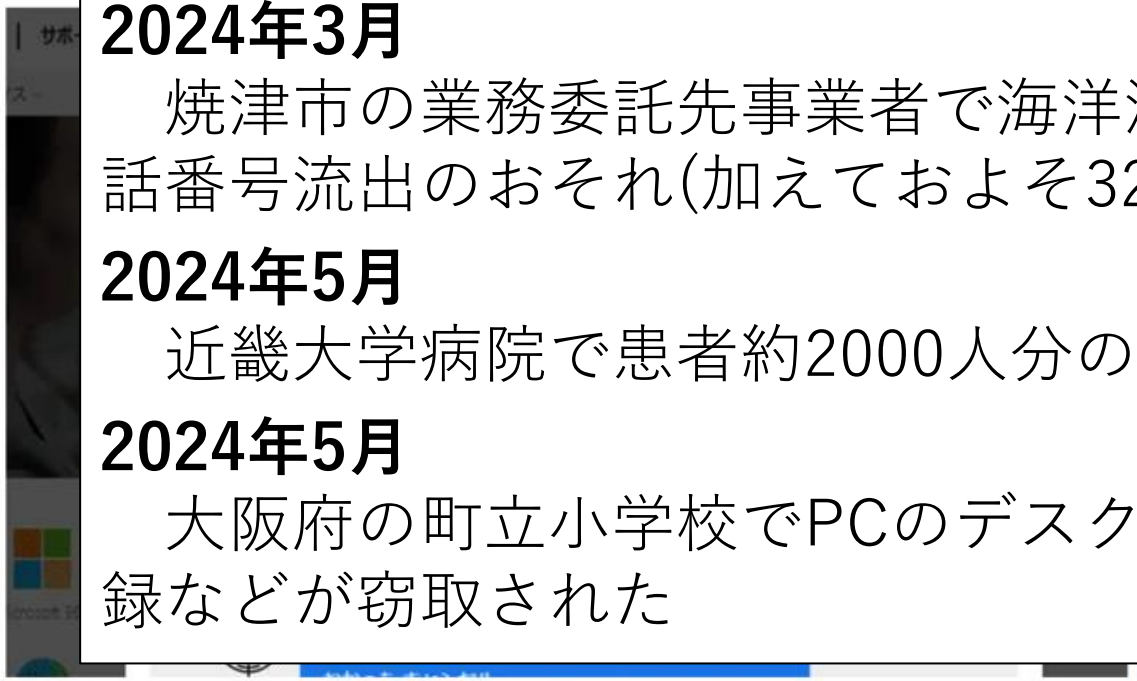
　焼津市の業務委託先事業者で海洋深層水購入者1万5000人分の氏名・住所・電話番号流出のおそれ(加えておよそ32万円も支払ってしまったとのこと)

2024年5月

　近畿大学病院で患者約2000人分の氏名・診察情報が流出のおそれ

2024年5月

　大阪府の町立小学校でPCのデスクトップデータが消失、児童約170人の指導記録などが窃取された



社外秘

2　最近のサイバー攻撃と、その手口

侮れない「サポート詐欺」の被害

一般的なWebサイトを閲覧中、急に「ウイルスに感染し[illegible]され、それに加えてPCの操作が著しく制限さ[illegible]

画面上にはMic[illegible]

これは詐欺です
絶対に電話をしてはいけません

[illegible]警告！

①サポート費用を請求されます

多くの場合、Amazonギフトカードなどのプリペイド式を指定してくるようです

②パソコンの操作を乗っ取られます

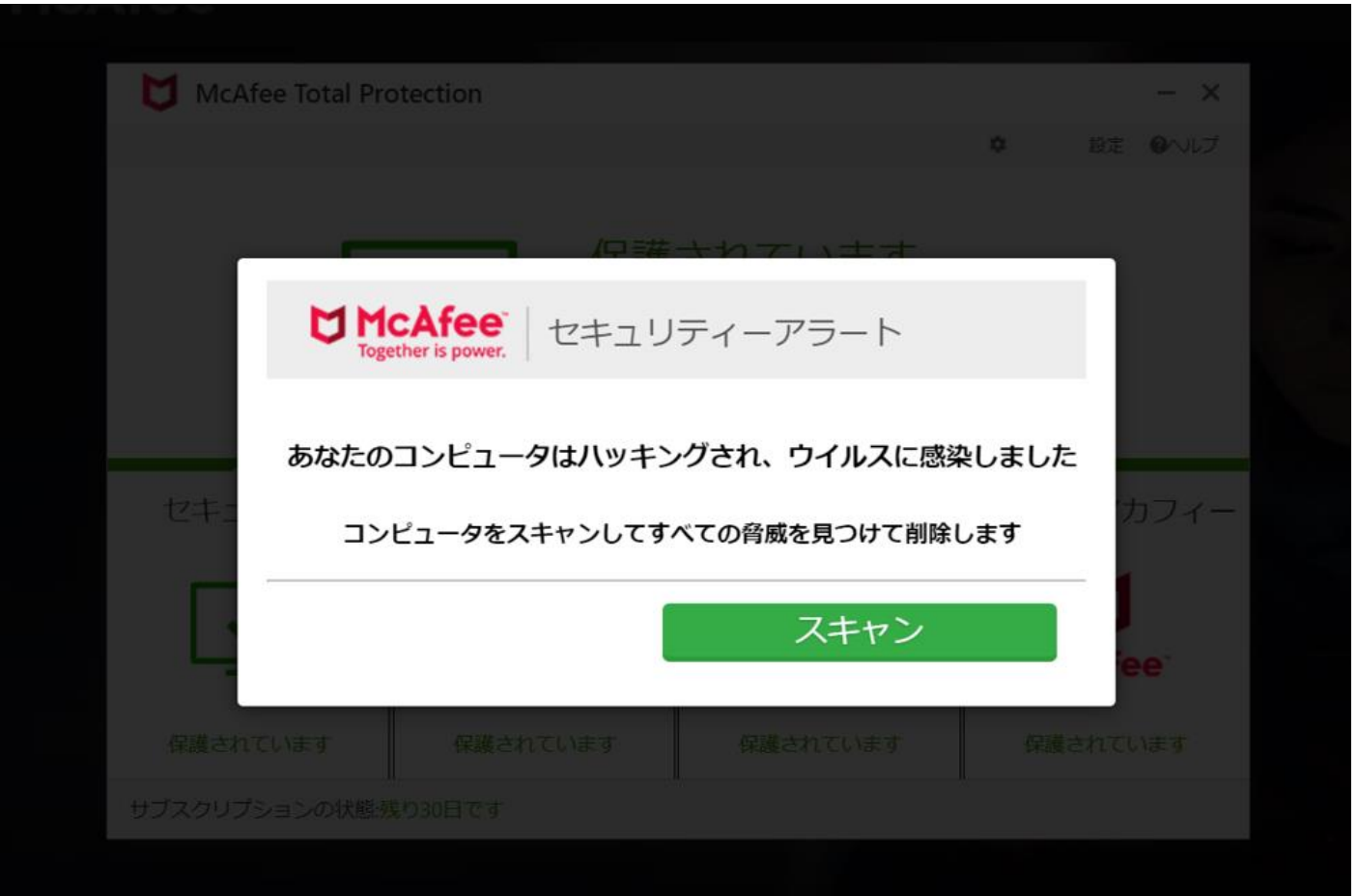
修復のため、などと称してリモートアクセスアプリをダウンロードさせるようです

社外秘

2　最近のサイバー攻撃と、その手口

変化を続けるサポート詐欺

最近では電話をさせないサポート詐欺も登場しているようです。



左の図もサポート詐欺ですが、クリックして進んでいくとウイルス対策ソフトの購入(更新)に見せかけた画面へたどり着くようです。

表示されているのは有名なウイルス対策ソフトの一つで、このメーカーのソフトをインストールしているPCで表示されたら、思わず購入しようとしてしまうかもしれません。

社外秘

2　最近のサイバー攻撃と、その手口

変化を続けるサポート詐欺

最近では電話をさせないサポート詐欺も登場して

これも詐欺です
絶対にお金を払ってはいけません

購入(更新)
たどり着くようです。

表示されているのは有名なウイルス対策ソフトの一つで、このメーカーのソフトをインストールしているPCで表示されたら、思わず購入しようとしてしまうかもしれません。

社外秘

2　最近のサイバー攻撃と、その手口

公社のウイルス対策ソフトのご紹介

　公社のPCには**トレンドマイクロ**社のウイルス対策ソフトをインストールしています。

　この製品以外のセキュリティ製品が表示された場合はサポート詐欺を疑いましょう。

ウイルスバスター動作中のイメージです

社外秘

3　サイバー攻撃に備えましょう

公社を狙ったサイバー攻撃なんて起こるの？

攻撃者が知っていること

〇公社は足立区の児童(と家族)に深く関わっている
　→**個人情報を狙われるかも**

〇公社は資産状況を公表している
　→**預金を狙われるかも**

攻撃者が知らないこと

〇公社は**足立区役所**とネットワークがつながってそう
　→本当はつながっていない他団体でも**侵入経路を探されるかも**

〇公社は区内の文化団体・施設の機密情報も持ってそう
　→本当は持っていない個人情報でも狙われるかも

社外秘

3　サイバー攻撃に備えましょう

ウイルス対策ソフトウェアが守ってくれる？

「ウイルス対策ソフトがあるから大丈夫」という考え方は、残念ながら正しくない場合があります。

【ウイルス対策ソフトウェアの働き】

○メーカーから配布されるシグネチャに合致するマルウェアを検知・除去

○公社のウイルス対策ソフトはサーバから毎時シグネチャを更新

○手動で即時ウイルスチェックも可能

シグネチャでマッチしたマルウェアは駆除します。

しかし、シグネチャ未登録のマルウェアは見逃してしまいます。

社外秘

出典：被害事例に学ぶ、今のサイバーセキュリティ実態と進化した対策の肝とは？(エムオーテックス社)

マルウェアは日々進行し、同じマルウェアは使われないことが多い

1日に作られるマルウェアの数

最近では誰でもマルウェアを作成出来ます。
企業のシステム環境は常に悪意のあるユーザーによって、**膨大なセキュリティリスク**にさらされていると言えます。

マルウェアの平均寿命

マルウェアは生まれてから、**58秒で消滅します。**
常に未知の新しいセキュリティリスクが生まれては消えています。

同じマルウェアが使われる割合

別の組織で再発見されるマルウェアは**たったの0.5%。**つまり、同じマルウェアが2度以上使われることはほとんどありません。
攻撃に使われる**マルウェアは、ほぼ"未知"であるといえます。**

VERIZON DBIR（データ漏洩/侵害調査報告書）2016の調査より

社外秘

3　サイバー攻撃に備えましょう

ウイルス対策ソフトウェアが守ってくれる？

「ウイルス対策ソフトがあるから大丈夫」という考え方は、残念ながら[illegible]場合があります。

【ウイルス対策ソフトウェアの仕[illegible]

○メーカ[illegible]　　を検知・除去

○[illegible]ごとに毎時シグネチャを更新

○[illegible]ルスチェックも可能

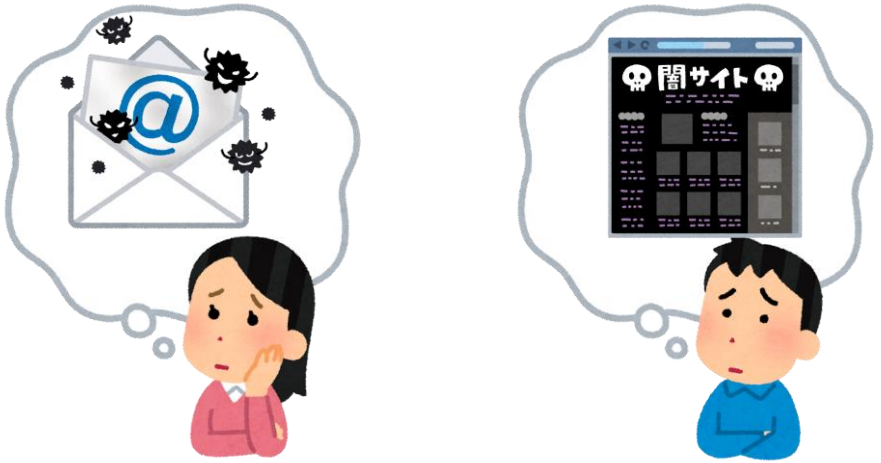
セキュリティに魔法なし！

シグネチャでマッチしたマルウェアは駆除します。

しかし、シグネチャ未登録のマルウェアは見逃してしまいます。

社外秘

３　サイバー攻撃に備えましょう



何に気を付ければいいの？

○不審なメールにご用心

　特に金銭に関係した話題ならば、担当者が実際に進行している案件かをしっかりと確認し、必要に応じてこちらから連絡しましょう。

　また、送信者とメールアドレスが一致しているか、にも注意が必要です。

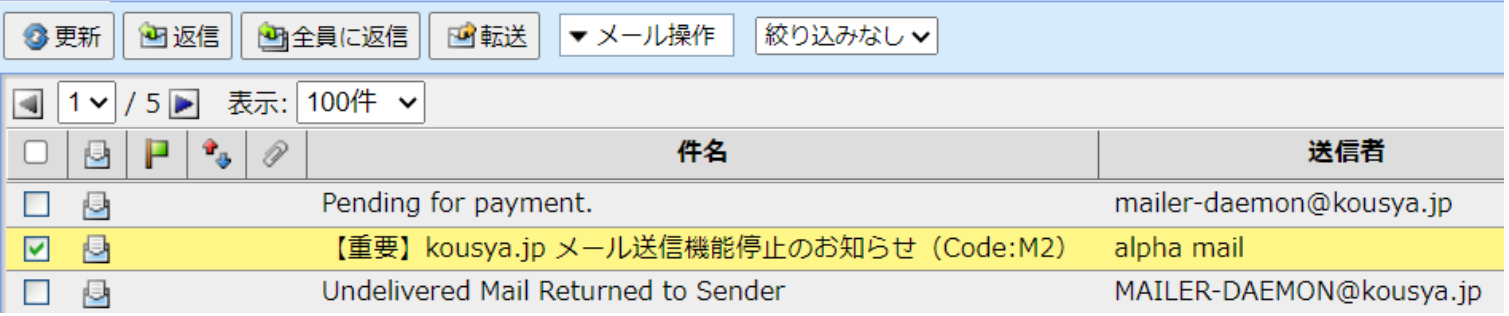
○怪しいURLは代わりにスキャンさせましょう

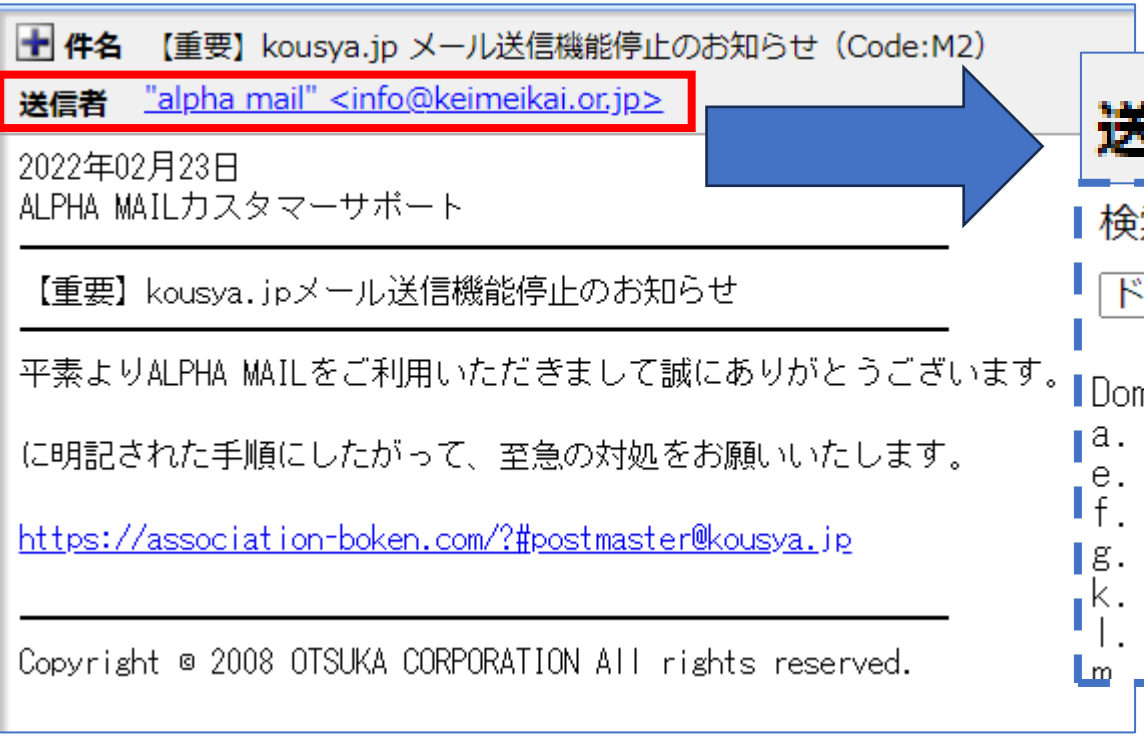
　公社ＰＣのブラウザには既定のお気に入りフォルダに「secURL」という代理アクセスしてくれるWebサイトを登録してあります。ぜひご活用ください。

○業務に関係ないWebサイトはなるべく閲覧しない

　i-FILTERも万能ではないので、閲覧できるWebサイトがすべて安全とは限りません。業務に関係のないWebサイトを頻繁に閲覧していると感染経路を増やすことになりかねません。

送信者の表示名を
そのまま信じると・・・





送信者欄に表示される名称は送り手が指定することができます
返信する前に、できればメールアドレスも確認しましょう

社外秘

３　サイバー攻撃に備えましょう

もしもサイバー攻撃に直面してしまったら

○不審なメールが届いたら

　メールは届いただけなら基本的に無害です。明らかに不審なメールが届いたら、そのままの状態にしておいて企画総務課までご報告ください。

○サポート詐欺が表示されたら

　サポート詐欺も表示された時点では原則無害です。まずは落ち着いてPCの背面からLANケーブルを抜き、速やかに企画総務課までご報告ください。

　絶対に表示されている電話番号にかけないでください。

○その他に「サイバー攻撃かも」と思ったら

　公社のネットワーク環境下では、サイバー攻撃はLANケーブルでのみ感染拡大が可能です。そのため、何かしらサイバー攻撃が疑われる事象がありましたらまずはLANケーブルを抜き、その後に企画総務課までご報告ください。

社外秘

3　サイバー攻撃に備えましょう

もしもサイバー攻撃に直面してしまったら

〇不審なメールが届いたら

　メールは届いただけなら、その

おかしいと思ったら
迷わずLANを抜け！！
（できれば優しく）

…までご報告ください。

…かないでください。

〇…に「サイバー攻撃かも」と思ったら

　公社のネットワーク環境下では、サイバー攻撃はLANケーブルでのみ感染拡大が可能です。そのため、何かしらサイバー攻撃が疑われる事象がありましたらまずはLANケーブルを抜き、その後に企画総務課までご報告ください。

社外秘

最後に

今回は近年激化の一途をたどるサイバー攻撃を簡単に紹介させていただきました。

公社もいつ被害者になるかもしれない世の中ですが、正しく備えて少しでも被害を軽微なものにできればと思っています。

まずは「何かおかしいと感じたら迷わずLANケーブルを抜く」にご協力をお願いいたします。

本動画は以上となります。

ご視聴ありがとうございました

最後にWebページから視聴アンケートを送信してください。

社外秘