公益財団法人 東京都医学総合研究所　御中

標的型攻撃メールの脅威と対応
最新情報セキュリティトピックス

2025年2月27日

株式会社ブロードバンドセキュリティ

本日のアジェンダ

1. 2024年度標的型攻撃訓練結果

- ✓ 標的型攻撃訓練実施結果

2. 標的型攻撃メールについて

- ✓ 標的型攻撃とは？

3. 最近の攻撃状況について

- ✓ IPA情報セキュリティ10大脅威 2024
- ✓ サイバー攻撃の事例と対策

4. 日頃から注意すべきセキュリティ対策ポイント

- ✓ セキュリティ対策ポイント①～⑪

各所からの注意喚起について

（警察庁、内閣官房内閣サイバーセキュリティセンター）

昨今のサイバー攻撃リスクの高まりを踏まえ、次々と注意喚起が出ています。

- ✓ MirrorFace（標的型メール）によるサイバー攻撃について (2025年1月8日) ※1
- ✓ 北朝鮮を背景とするサイバー攻撃グループTraderTraitor によるサイバー攻撃について(2024年12月24日) ※2
- ✓ サイバー警察局便りR6Vol.7「ランサムウェア被害は高水準で推移！」 (2024年9月6日) ※3
- ✓ サイバー警察局便りR6Vol.3「そのメール、フィッシングかも！」 (2024年6月25日) ※4

リスク低減のための措置

✓ **マルウェア感染リスクの低減**	添付ファイルを不用意に開かない、本文内URLを不用意にクリックしない、連絡・相談を迅速に行う。
✓ **アカウント管理徹底による認証強化**	安全なパスワード設定の周知徹底、アクセス権限の適切な制御、多要素認証の利用等。
✓ **脆弱性管理の徹底**	IoT機器を含む情報資産（VPN装置やゲートウェイ等、インターネットとの接続を制御する装置）のセキュリティパッチ（最新のファームウェアや更新プログラム等）の迅速な適用による、脆弱性管理の徹底を進め、**アタックサーフェスの防御**を実現する。

※1：警察庁サイバー警察局、内閣ｻｲﾊﾞｰｾｷｭﾘﾃｨｾﾝﾀｰより https://www.npa.go.jp/bureau/cyber/koho/caution/caution20250108.html
※2：警察庁サイバー警察局、内閣ｻｲﾊﾞｰｾｷｭﾘﾃｨｾﾝﾀｰより https://www.npa.go.jp/bureau/cyber/koho/caution/caution20241224.html
※3：警察庁より https://www.npa.go.jp/bureau/cyber/pdf/R6_Vol.7cpal.pdf
※4：警察庁より https://www.npa.go.jp/bureau/cyber/pdf/R6_Vol.3cpal.pdf

1．2024年度標的型攻撃訓練結果

標的型攻撃訓練実施結果

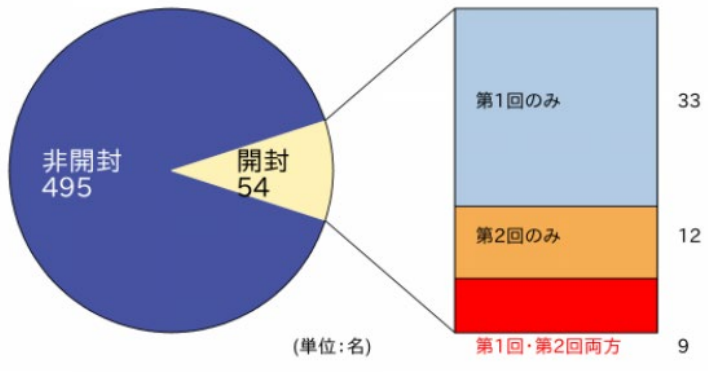
実施概要

第1回訓練 2024年09月17日　ファイル添付型
第2回訓練 2024年11月06日　URL型

開封率

年度	開封率
2024年	9.8%
2023年	8.2%
2022年	21%
2021年	28%
2020年	8%
2019年	33%

開封者の内訳



- 50人以上がメールの添付ファイル・リンクを開封。
- 昨年度より第1回、第2回両方開封した人が増加。

URLへアクセス/添付ファイルを開いてしまう理由

開封理由

- ✓ 自分の業務と関連がある内容だったため
- ✓ 興味ある内容だったため。

- ● 他人事ではなく、状況によっては**自身にも起こり得る**と捉える
- ● 開かなかった人も訓練の一環で**開けてしまったときの対応を再確認**

訓練実施結果を踏まえた注意点

開封者数

1回目開封者：**42人**

2回目開封者：**21人**

報告者数

1回目の報告者：**13/42人**

2回目の報告者：**4/21人**

- 開封者に対し、報告した人の数が少ない
- ネットワーク切断、情報セキュリティ責任者への**報告までが訓練**

  →感染などで端末が使用不可になっても、報告先はわかるようになっているか？
- 報告しなくても問題ないという**独自判断は大変危険**

  →判断がつかないときには**「まず報告」**するのが正しい

訓練だとわかっても必ず庶務係に報告してください

不審なメールのURLや添付ファイルを開いたら報告するのが所内ルール

訓練実施結果を踏まえた注意点

- 攻撃者は**次々と新たな方法で**攻撃をしかける
  - ✓ 攻撃者の**攻撃手法、傾向、対応**を学ぶ
  - ✓ 攻撃が世界中で多発していると**日々意識する**こと
- 攻撃者は目的をもって攻撃をしかける**プロ**である
  - ✓ 愉快犯などではなく**金銭目的のビジネス**
  - ✓ **早期に攻撃と気づける**ことが大事
  - ✓ 実態を把握して対応するためにも**適切な報告が必要**

2. 標的型攻撃メールについて

標的型攻撃メールの特徴

標的型攻撃メールとは

標的型攻撃メールとは、特定の個人や組織を狙って送られる不正なメールのことです。攻撃者は、送信者を偽装したり、業務に関連する内容を装って受信者を信用させ、悪意のあるリンクをクリックさせたり、添付ファイルを開かせたりします

特徴

- 差出人の名前やアドレスが見慣れない
- 組織内の話題にも関わらず外部のメールアドレスから届いている
- URLをクリックするように誘導している
- ファイルの添付があり、開くよう誘導している
- 緊急！至急！重要！と見出しをつけ、添付ファイルを開かせようとする
- 差出人の署名や名乗りが無いか曖昧である
- 本文の日本語がおかしい、または日本では使用されていない漢字がある
- 発信元がフリーメールである

リンクや添付ファイルを開いてしまうと・・・

マルウェア感染

リンクや添付ファイルを開くことで、ウイルス、トロイの木馬、ランサムウェアなどのマルウェアがPCに侵入し、システムが感染する恐れがあります。

フィッシングサイトへの誘導

偽のログインページや企業の公式サイトに似せたページに誘導しユーザIDやパスワードなどの認証情報を入力させます。

情報流失、マルウェアによる業務停止などにより金銭的な損失や社会的信用の失墜を招くことになります。

標的型攻撃メールのタイプ

URLリンク型

メール本文中にURLリンクを記載し
不正サイトに誘導するタイプ

添付ファイル型

PDF、Word、Excelなどの実行ファイルを添付するタイプ

何も添付しない型

主に「やりとり型攻撃」に使用
相手が信用した後にURLやウイルスファイルを送りつけるタイプ
※初期偵察の目的の場合もある

URLリンク型の例

標的型攻撃メールの手口（URLへの細工）

1．短縮URL

サーバ転送技術を使用し、転送先を隠す

（例）
http://bit.ly/1gPmXic

対策

bit.ly、J.mp等の短縮URLは、末尾に**+**を付け、確認ページでチェック

（例）
http://bit.ly/1gPmXic+

2. 偽物URL

正規のサイトに見せかける

（例）
www.jal.co.jp.cn/reservation.html

対策

記載されたURLに不自然な点がないか確認。確認サイト活用も有効

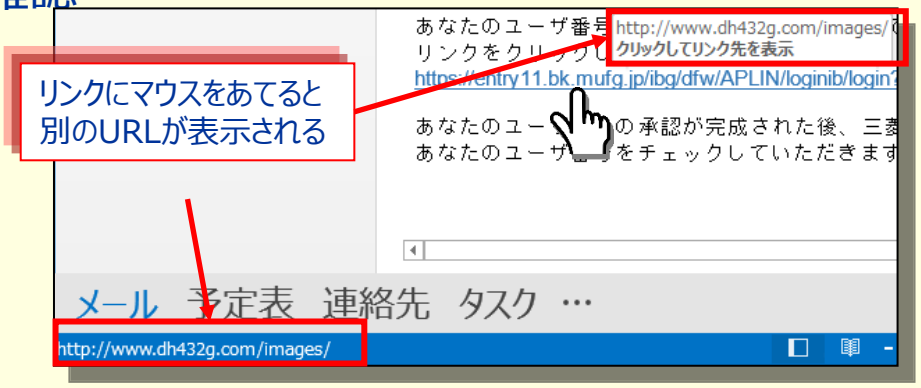
（確認サイト例）
https://www.aguse.jp/
https://www.urlvoid.com/

3．HTMLメール①

表示されているURLと実際のリンク先が異なる

対策

URL上にマウスカーソルを合わせ、遷移先のURLを確認



4．HTMLメール②

具体的なURLが表示されていない

（例）
詳細は、こちらを確認

標的型攻撃メールの手口（添付ファイルへの細工）

1．ファイル拡張子の細工

exeファイルの見た目

- **二重拡張子**　abc.doc.exe

  拡張子を表示しない設定により「abc.doc」と表示

- **空白文字挿入**　abc.pdf　　.exe

  大量の空白により「.pdf」以降が表示されない

- **左右逆転表示**　exe.abc.doc

  文字制御（Right-to-Left Override）悪用

- **ショートカットファイル**（.lnk）

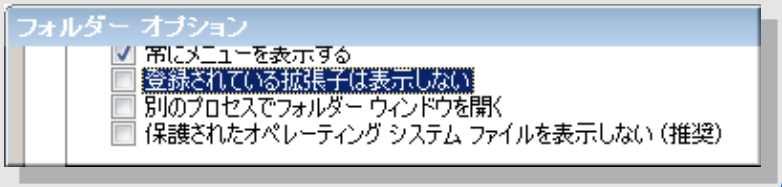
  スクリプトの埋め込みが可能

2．圧縮ファイル+パスワード

Zipファイルにパスワードをかけることでウイルス対策ソフトをすり抜ける

日本製フリーソフト「アタッシェケース」の使用事例も

フォルダオプションで「登録されている拡張子は表示しない」のチェックを外す



対策

1．不審な添付ファイルは、**開く前に「メール以外の方法で」送信元に問い合わせ**を行う

2．ファイルの**拡張子を表示**させ、ファイルの属性を確認する

標的型攻撃メールの手口（アイコン偽装）

手口

添付する実行ファイルのアイコンを別のアイコンに変更しクリックさせる

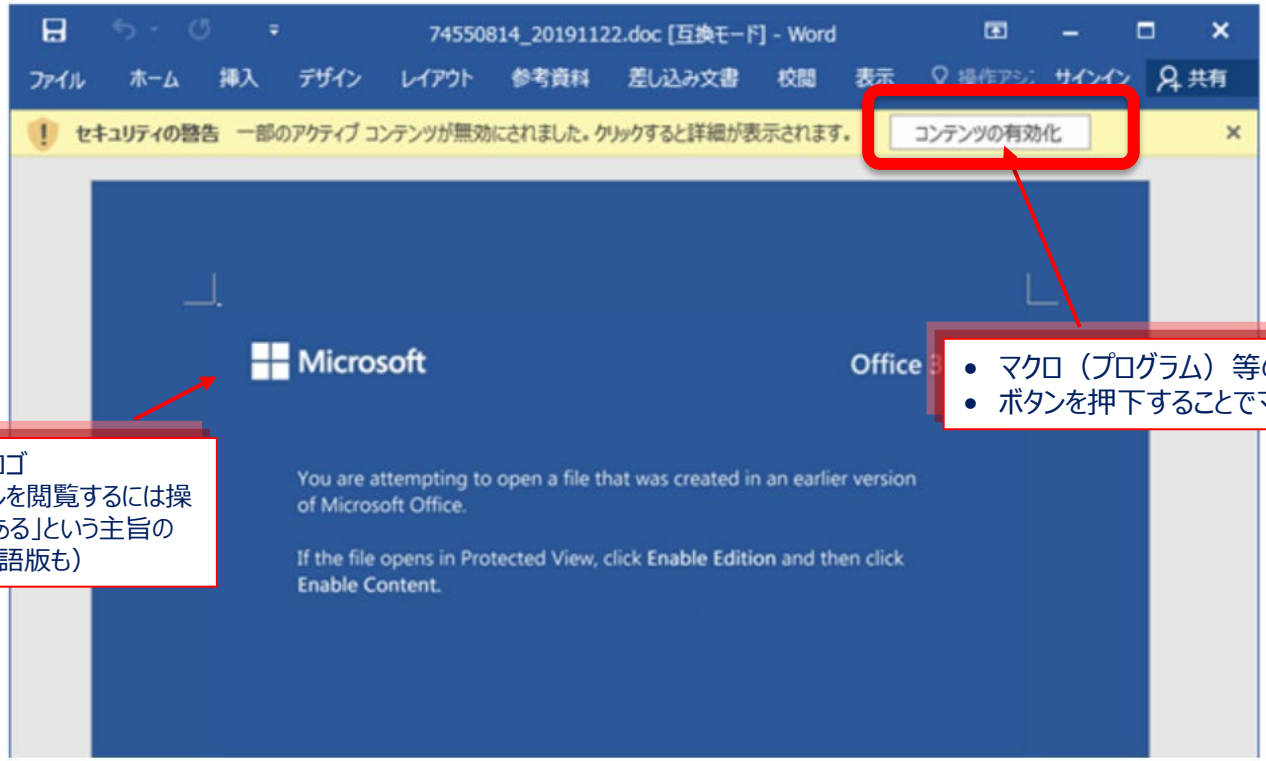
感染までの流れ

対策

・ファイルの拡張子を確認する
・デスクトップには保存せずフォルダへ保存する
（デスクトップ上では、ファイル名がすべて確認できないため）

標的型攻撃メールの手口

添付ファイルを開いた時の画面例



- Office等のロゴ
- 「文書ファイルを閲覧するには操作が必要である」という主旨の文面（日本語版も）

- マクロ（プログラム）等の実行を許可するという意味のボタン
- ボタンを押下することでマクロが動作し、ウイルスに感染

標的型攻撃メール対策まとめ

- 送信元アドレスの確認

  →正規のアドレスから届いているか？組織内のメールなのに外部のメールアドレスから届いていないか？

- メール内のURLリンクや添付ファイルをむやみに開かない

  →URLリンクに不自然な点がないか？添付ファイルの拡張子は正しいか？

- メールの件名や本文が不自然でないか

  →件名に緊急・至急・重要などがないか？本文の日本語は正しいか？

- もし不審なメールのURLや添付ファイルを開いてしまったら・・・

  すぐに情報セキュリティ責任者経由で情報システム室・庶務係に報告！
  ※所内ルールです

標的型攻撃メールと誤解されないために

標的型攻撃メールとの差別化

① 具体的な件名をつける（Re:Re:〇〇、などではなく）

② 相手の名前、自分の名前を明記する（不審メールには無い）

③ 具体的な日時/内容を明記する（昨日の〇〇の件のご回答、など）

④ メールに添付ファイルではなく、クラウドでのデータ受け渡しにする

⑤ メール件名に【重要】など標的型メールに似た文言を入力しない※

⑥ 署名は必ず入れる（名刺と記載を変えて略称にするなどもあり） **※**

※⑤、⑥は所内ルールとなります。誤解されないためにも必ず実施してください

3. 最近の攻撃状況について

情報セキュリティ10大脅威 2024

IPA 情報セキュリティ10大脅威 2024

昨年順位	個人	順位（組織）	組織	昨年順位
8位	インターネット上のサービスからの個人情報の窃取	**1位**	ランサムウェアによる被害	1位
9位	インターネット上のサービスへの不正ログイン	**2位**	サプライチェーンの弱点を悪用した攻撃	2位
4位	クレジットカード情報の不正利用	**3位**	内部不正による情報漏えい等の被害	4位
5位	スマホ決済の不正利用	**4位**	標的型攻撃による機密情報の窃取	3位
7位	偽警告によるインターネット詐欺	**5位**	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	6位
2位	ネット上の誹謗・中傷・デマ	**6位**	不注意による情報漏えい等の被害	9位
1位	フィッシングによる個人情報等の詐取	**7位**	脆弱性対策情報の公開に伴う悪用増加	8位
6位	不正アプリによるスマートフォン利用者への被害	**8位**	ビジネスメール詐欺による金銭被害	7位
3位	メールやSMS等を使った脅迫・詐欺の手口による金銭要求	**9位**	テレワーク等のニューノーマルな働き方を狙った攻撃	5位
10位	ワンクリック請求等の不当請求による金銭被害	**10位**	犯罪のビジネス化（アンダーグラウンドサービス）	10位

（出典）独立行政法人情報処理推進機構セキュリティセンター（IPA）「情報セキュリティ10大脅威2024」 https://www.ipa.go.jp/security/10threats/10threats2024.html

セキュリティインシデントの傾向

2024年に発生したインシデントの傾向

- メール（添付ファイルや本文中リンク）からの**ランサムウェア感染**による攻撃
- ネットワーク機器（VPN装置）の**脆弱性を突いての攻撃**
- 公開サーバやクラウドの設定不備、Webサーバの**脆弱性を突いての攻撃**
- **内部からの脅威**（従業員/派遣社員などによるデータ漏えいや不正アクセス）

2024年中の具体的事例

発生日	発生企業	事件概要
2025年2月	イズミ	ランサムウェア感染による業務停止、最大で778万4999件の個人情報情報流失
2025年5月	イセトー	ランサムウェア感染による業務停止、少なくとも約150万件の個人情報が流出
2025年6月	KADOKAWAグループ	ランサムウェア感染による業務停止、約25万件の個人情報が流出
2025年7月	東京ガスエンジニアリングソリューションズ	ネットワークへの不正アクセスにより、約416万人の個人情報が流出

セキュリティインシデントの傾向

サイバー攻撃被害額（過去3年間）

- サイバー攻撃を受けた法人1社あたりの平均被害額
  →1億7,100万円（前年より約4,600万円増加）

- ランサムウェア攻撃を受けた法人1社あたりの平均被害額
  →2億2,200万円（前年より約4,400万円増加）

費用の具体的な内訳

事故対応費用	初動対応、調査（フォレンジック）など
事後対策実施費用	脆弱性対策などの実施費用
賠償費用	情報漏えい時の賠償、弁護士費用
行政支払費用	法令違反による罰金、課徴金

※その他、ブランドイメージの低下、株価の下落など金銭的換算が困難な損害も発生

①ランサムウェアによる被害（KADOKAWAグループ ）

経緯

2024年6月8日に、「ニコニコ動画」など、KADOKAWAグループの複数のウェブサイトなどで障害が発生してサービスが停止する事件が発生。ランサムウェアを含む大規模なサイバー攻撃が原因であると発表。
その後ランサムウェア攻撃グループによる情報漏洩が確認した。

時系列

2024年6月8日	大規模サイバー攻撃発生。複数のシステムが停止する。
2024年6月14日	被害を受けた動画配信サービスからプレスリリース公開。ランサムウェアを含む大規模なサイバー攻撃であることを公表。
2024年6月28日	ランサムウェアグループによる情報漏洩が確認され、それを受けたプレスリリースが公表される。
2024年7月2日	さらなる情報漏洩が確認され、それに伴うプレスリリースが公表される。

被害状況

データセンター内に構築されたプライベートクラウドが攻撃を受け、仮想マシンが暗号化された。
感染が拡大しないよう、データセンターのすべてのシステムをシャットダウンしたが、攻撃者が遠隔による起動・感染拡大を試みてきたため、これを防ぐために物理的にケーブルを引き抜いて対応。
その影響でKADOKAWAグループが提供する複数のサービスが影響を受け、その後情報漏洩が確認された。

ランサムウェア対策

- 不審なメールの添付ファイルやリンクは開かない。送信元を確認し、不明な送信者からのメールは削除する。
- 強力なパスワードを設定し、定期的に変更する。使い回しをしない。
- OSやアプリケーション、ウイルス対策ソフトを定期的に更新する。
- 重要データは社内ルールに従いバックアップを取る。
- 社内セキュリティポリシーの遵守許可されたソフトウェア・デバイスのみ使用する。
- 公共Wi-Fiを避け、社内ネットワークやVPNを利用する。
- 異常を感じたらすぐに報告PCの動作が不審な場合や、怪しいメールを受け取った場合は速やかにIT部門へ報告する。

②内部不正による情報漏えい（兼松）

経緯

大手総合商社の双日の元社員（32）が2024年9月28日、前職で勤めていた総合商社の兼松から機密情報を含むデータファイル不正に持ち出した不正競争防止法違反の容疑で逮捕された。

時系列

- 元社員が前職の同僚の女性派遣社員に対して「海外出張先の飲食店リストが欲しい」とうその説明をして、サーバーへ接続するために必要なIDなどを聞き出し犯行に及んだ。
- 同派遣社員は男にログインに必要なID、パスワードに加え確認コードも伝えていた
- 元社員は、兼松の従業員の多くが休む週末（土日）にデータベースに対してアクセスを繰り返しており、単一アカウントから多数のアクセスが行われていたことが異常として検知された。

被害状況

- 元社員は、兼松が管理する海外の自動車部品メーカに向けた新製品の提案書や採算表などの 営業秘密を不正に入手。元従業員による営業秘密の不正利用や第三者に対する漏えいなどは確認されていない。
- 兼松は元社員が退職直前に兼松が利用しているオンラインストレージサービスから3万7000件のファイルをダウンロードしていた形跡が確認されており、警視庁はこれらが営業秘密に該当するか捜査している。

内部不正対策

- 情報の取り扱いルールを守り、業務データの無断持ち出しやコピーをしない。
- 強力なパスワードを設定し、定期的に変更する。使い回しをしない。
- 業務情報をSNSや個人メールで送信しない。
- 許可されたデバイス以外を使用しない。
- 退職・異動時に業務データを個人的に持ち出さない。
- 内部不正が企業や同僚に与える影響を理解し、正しい行動を心がける。
- 従業員が働きやすい環境を整え、ストレスや不満を軽減することで不正行為を抑制する。

③フィッシング詐欺

フィッシング詐欺とは？

フィッシング詐欺は、銀行・クレジットカード会社・通販サイトなどになりすまして偽のメールやSMSを送り、個人情報（ID・パスワード・クレジットカード情報など）を盗み取る詐欺 です。

最新の状況

- 2024年12月の報告件数：

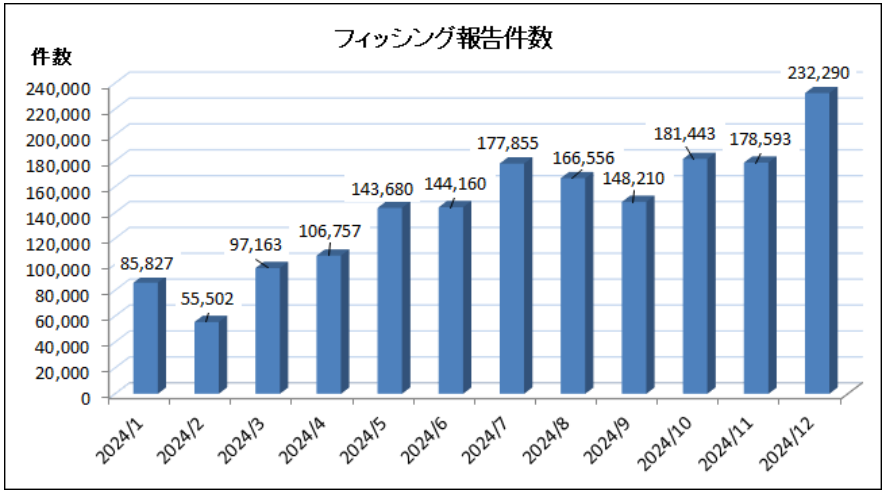
232,290件（前月比 30.1%増）

※フィッシング報告数・URL数は過去最高を記録

- フィッシング手口の傾向

① Amazon、えきねっと、PayPay、佐川急便、国税庁、クレジットカード各社などを装う

② 「不正使用検知」、「支払い情報変更」、「ポイントプレゼント」などの内容



出典：https://www.antiphishing.jp/report/monthly/202412.html
フィッシング対策協議会「2024/12 フィッシング報告状況」 より

③フィッシング詐欺

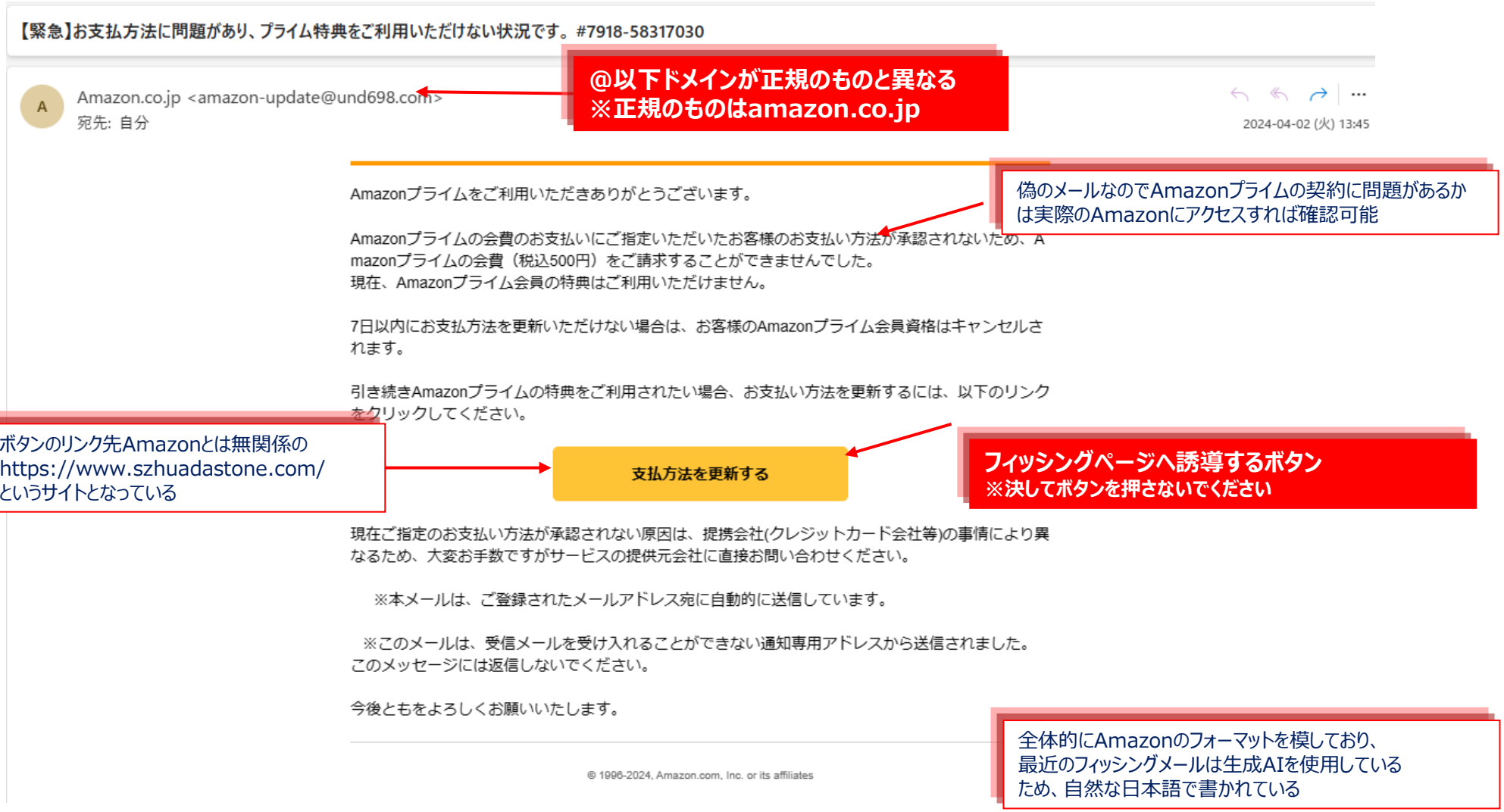
攻撃手法

- ビッシング（音声フィッシング） ➡ 偽の公的機関や企業を名乗り、電話で金銭や個人情報を要求
- スミッシング（SMSフィッシング） ➡ SMSで偽のリンクや電話番号を送り、情報を盗む
- クイッシング（QRコードフィッシング） ➡ QRコードに偽サイトのリンクを埋め込み、情報を入力させる
- モバイルフィッシング（メール型） ➡ スマホで開いたときだけ動作する巧妙なフィッシングメール

対策方法

- 自分の名前が記載されているかチェック（対策の一環として名前を記載する企業が増えている）
- 通常と異なるアドレスのメールは注意
- メール内URLリンクからではなく、**公式アプリや正規サイトから直接ログインを確認**
- ログイン不可などがあれば、すぐに公式サポートへ連絡しアカウント停止を依頼

事例（1） Amazonを騙った事例



@以下ドメインが正規のものと異なる
※正規のものはamazon.co.jp

偽のメールなのでAmazonプライムの契約に問題があるかは実際のAmazonにアクセスすれば確認可能

ボタンのリンク先Amazonとは無関係の
https://www.szhuadastone.com/
というサイトとなっている

フィッシングページへ誘導するボタン
※決してボタンを押さないでください

全体的にAmazonのフォーマットを模しており、
最近のフィッシングメールは生成AIを使用しているため、自然な日本語で書かれている

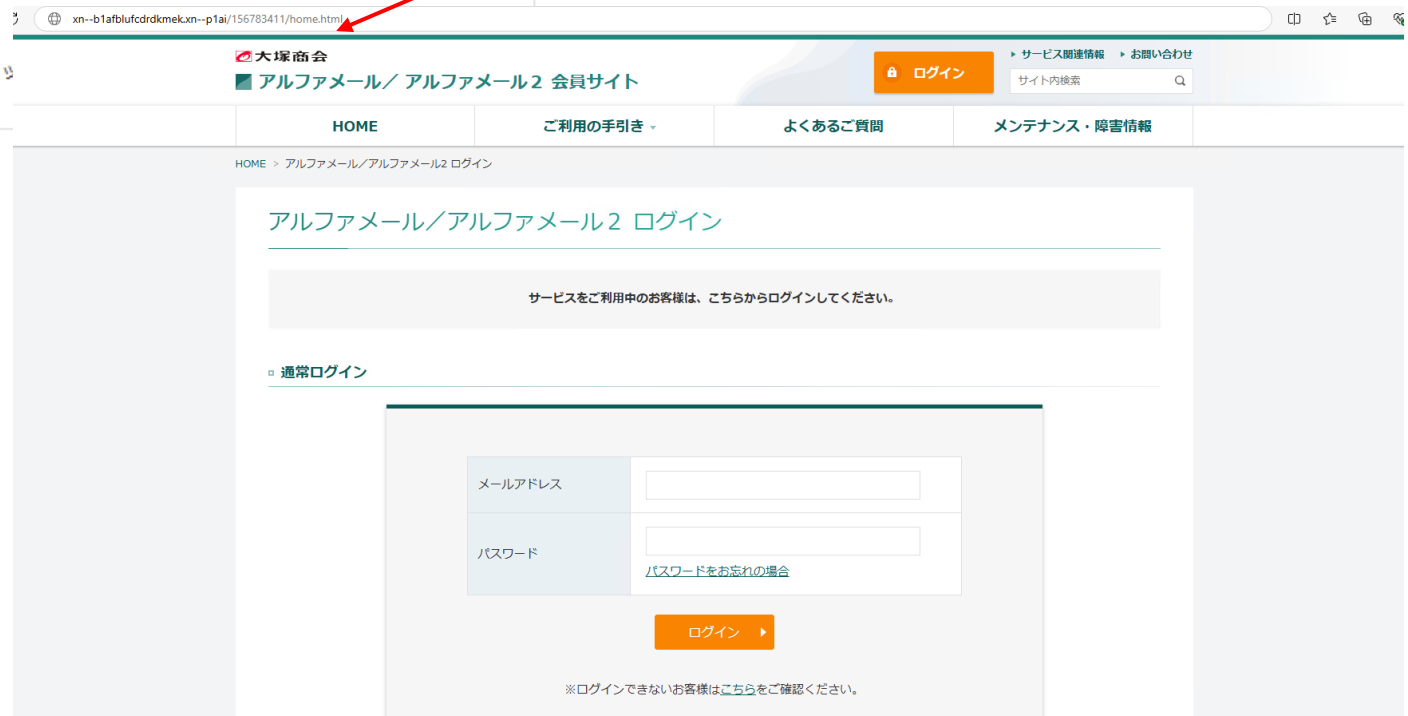
事例（2） 大塚商会のサービスを騙った事例

件名	【アルファメール２】パスワード再設定URLのご案内
送信元	Administrator
本文	**お客様メールアドレス** に割り当てられたパスワードは、本日**YYYY**年**MM**月**DD**日**曜日**に期限切れになります。 同じ設定を有効にするには、次のリンクをクリックします。 （偽サイトへのリンク） これはシステムによって生成されたメッセージです。

フィッシングページへ誘導するボタン

正規の大塚商会のサービスと全く同じログイン画面が表示されるがURLが正規のものと異なる。

偽サイトへのリンクをクリックすると・・・
※検証のため安全な環境でリンクをクリックしています。決してボタンを押さないでください。



④サポート詐欺

概要

インターネットを利用している際に、偽のウイルス感染警告やセキュリティ警告が表示される手口です。これにより、ユーザーの不安を煽り、表示された電話番号に連絡させることで金銭を騙し取る詐欺です。
弊社のお客様からもサポート詐欺に関するお問い合わせが増えています。

サポート詐欺の手口

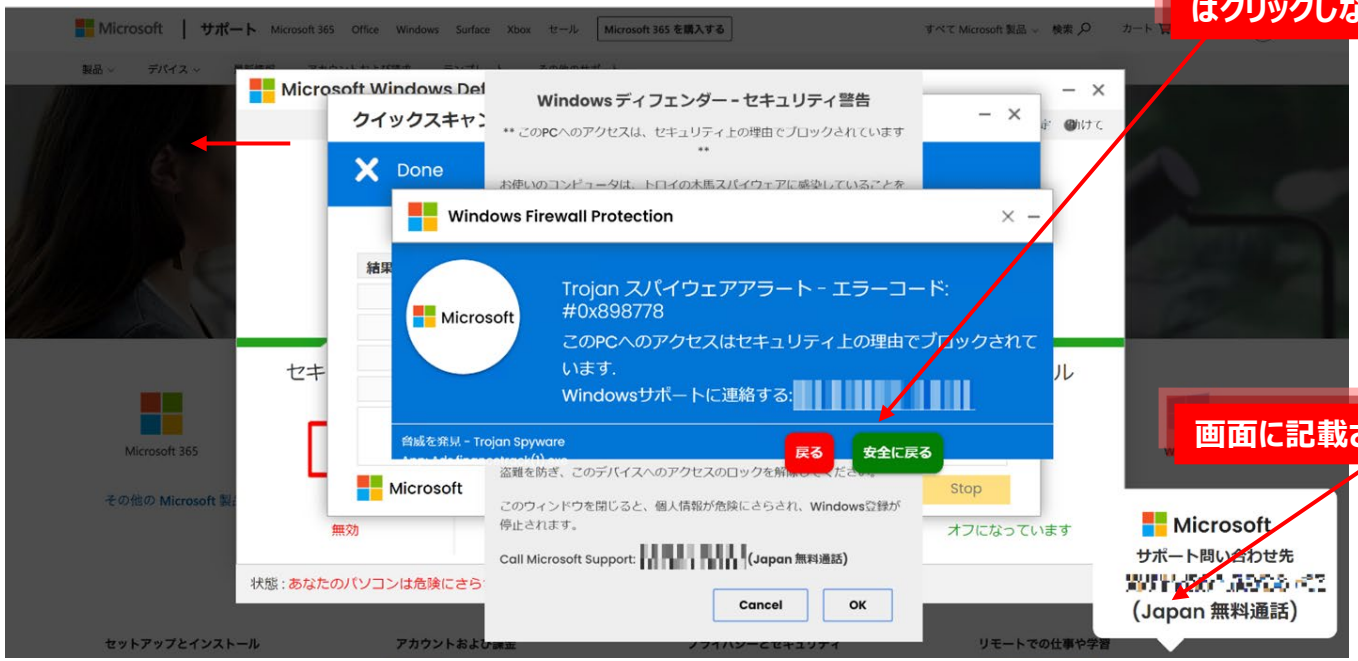
- **偽の警告表示:** ユーザーがウェブサイトを閲覧中に、「ウイルスに感染しました」「個人情報が漏洩しています」といった警告が表示されます。この警告には、サポートセンターの電話番号が記載されており、ユーザーはその番号に電話をかけるよう促されます。

- **金銭の要求:** 電話をかけると、「ウイルスを除去するために〇万円が必要です」といった形で金銭を要求します。また、遠隔操作ソフトのインストールを促し、実際にユーザーのコンピュータを操作して高額なサポート料金を請求することもあります。

- **不正な情報の取得:** 遠隔操作ソフトをインストールさせ、ユーザーの個人情報や金融情報を不正に取得します。

④サポート詐欺

サポート詐欺の画面例



サポート詐欺の画面に表示されているボタンはクリックしない

画面に記載されている番号に電話をしない

対処法

パソコンにこのような画面出たら、対処を自分一人で判断せず、会社・組織の対応ルールに従い、落ち着いて情報セキュリティ責任者経由で情報システム室・庶務係に連絡してください。

各業界のセキュリティ方針と取り組み①

各業界の主要なガイドラインの目的

- 自動車：自動車産業全体のサイバーセキュリティ対策のレベルアップや対策レベルの効率的な点検を推進
- 医療　：医療情報システムの安全管理や情報通信の技術の利用に関する法律等への対策
- 教育　：教育情報セキュリティポリシーの考え方および内容について解説

ポイントは外部ネットワーク接続の有無

- 自動車：ITインフラ環境や工場等の制御システムをはじめとして企業が管理する多くの情報システム
- 医療　：外部の医療機関等や患者自身などと医療情報の共有や連携、医療情報の外部保存を行うシステム
- 教育　：学校ホームページや教職員によるメールの活用、学習活動に使用されるシステム

各業界のセキュリティ方針と取り組み②

自動車

サプライチェーンリスクの高い業種として国土交通省の認証制度や経済産業省のフレームワークで要請を受けて業界ガイドラインを作成

より具体的な期間や基準といった明確なビジョンが示されており、セキュリティガイドライン準拠が推進されている

すでに業界全体のIT化が浸透しており、どのくらいセキュリティ対策が実施されているかが問われているステージ

医療

取り扱う情報の特殊性から「医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス」の理解もあわせて求められている

ガイドライン改定版の主眼は読みやすさであり、実効性を高める工夫に重点が置かれている

システム運用専任者なし、カルテ管理が紙媒体といった組織もある中、IT環境に関らず、まずは安全管理体制の構築が主眼のステージ

教育

2017年版のセキュリティガイドライン策定の結果、その遵守にとらわれるあまり教育情報活用推進の弊害となったことへの懸念表明あり

IT導入は進んでおり、地域格差も縮まっているが、業界全体としてのセキュリティ実態は見えづらく、IT活用状況についての調査結果が多い

システム活用自体が発展途上であり、セキュリティ対策よりはIT導入推進が主眼のステージ

参考情報：

https://www.jama.or.jp/operation/it/cyb_sec/docs/cyb_sec_supply_chain_CS_guide_2022.pdf
https://mhlw-training.saj.or.jp/wp/wp-content/uploads/2023/02/01-mhlw.pdf
https://www.mext.go.jp/content/20220304-mxt_shuukyo01-100003157_1.pdf
https://www.mhlw.go.jp/content/10808000/001102570.pdf
https://www.jama.or.jp/operation/it/cyb_sec/docs/cyb_sec_guideline_V02_01.pdf
https://www.mext.go.jp/content/20221027-mxt_jogai02-000025395_100.pdf

5. 日頃から注意すべきセキュリティ対策ポイント

日頃から注意すべきセキュリティ対策ポイント①

ガバナンス・リスク管理

- 情報セキュリティ関連規程を確認し、**規定を遵守した業務**を行う。
- クラウドサービスは、**定められたルールの範囲でのみ**利用する。
- ルール上は明文化されておらず、技術的に可能な利用方法について、**暗黙的に許可されていると解釈せず**、利用是非についてシステム・セキュリティ管理者に確認する。

※会社が許可したクラウドサービス以外の利用は禁止

日頃から注意すべきセキュリティ対策ポイント②

資産・構成管理

- 業務端末が**企業等として守るべき情報資産**に該当することを認識して適切に管理し、盗難・紛失防止に努める。
- 業務端末にアプリケーションをインストールする際は、**ルールで許可されたもの**（システム・セキュリティ管理者に申請し許可を受けたものを含む）のみをインストールする。
- インストールが許可されたアプリケーションについて、公式アプリケーションストア、ベンダーの公式HPなど**定められた場所からのみダウンロード**してインストールする。

※会社が許可したアプリケーション以外のインストールは禁止

日頃から注意すべきセキュリティ対策ポイント③

脆弱性管理

- 業務端末におけるOSをはじめとしたソフトウェアについて、自動アップデートを有効にするなど**アップデートを適切に実施**する（Windows8やFlash Playerなどサポートが終了した製品を使用しない）。
- 外出先で使用する無線LANルータ等の機器についても、**ファームウェアを最新版に更新**する。
- 業務端末のうち、特にスマートフォンやタブレットに関して、**不正な改造を実施しない**。

※OSやアプリケーションの最新のセキュリティパッチを適用

日頃から注意すべきセキュリティ対策ポイント④

データ保護

- 業務で取扱う情報は、利用者・保管場所・利用可能なシステム環境の要件など**定められた取扱方法に従って**取扱う。
- リムーバブルメディア（USBメモリ、CD、DVD等）は、**ルールで許可されており、業務上必要な場合のみ**利用する。
- 業務端末にデータを保存することが想定される場合は、内蔵されるHDDやSSDの**記録媒体レベルでの暗号化**を実施する。

※業務データの持ち出し時に多数の流出事故が発生している

日頃から注意すべきセキュリティ対策ポイント⑤

マルウェア対策

- 少しでも不審を感じたメール（添付ファイルやURLリンク等を含む）は開かず、必要に応じて**メール以外の手段で送信者に送信状況の確認を行う**ほか、システム・セキュリティ管理者へ速やかに報告する。報告の是非について判断に迷う場合は報告することを心がける。
- 業務端末には必ず**セキュリティ対策ソフト（ウイルス対策ソフト）をインストール**し、定義ファイルの自動更新やリアルタイムスキャンが行われるようにする。

※必ず最新のアンチウイルス定義ファイルに自動更新

日頃から注意すべきセキュリティ対策ポイント⑥

通信の保護・暗号化

- クラウドサービス接続時やデータ送受信を行う際は、**通信経路が暗号化**された方法（VPN、TLS等）を利用する。
- 無線LANルータ等の機器を利用する場合は、無線LANのセキュリティ方式として**「WPA2」または「WPA3」を利用**し、**暗号化のためのパスワードは第三者に推測されにくいものを利用**する。
- クラウドサービス（メール、チャット、オンライン会議、クラウドストレージ等）を利用する場合、**接続先のURLが正しいこと**（偽サイトでないこと）を確認した上で利用する。

※業務における公衆の無線LAN接続は禁止

※個人Wi-Fi、私用スマホによるモバイルルータ/テザリングは更新必須

日頃から注意すべきセキュリティ対策ポイント⑦

アカウント・認証管理

- 業務ネットワーク接続に必要となる**利用者認証情報（パスワード、ICカード等）を無断貸与や紛失等しない**よう、適正に管理する。
- **パスワードは、第三者に推測されにくいものを設定**する。多くの文字数/文字種を設定できる場合は、大文字/小文字/数字/記号を組み合わせるなどして、文字数が長いものを設定する。
- 複数のサービス間で**同じパスワード使い回さない**。また、使用するパスワードが第三者に知られた可能性がある場合は、早急にパスワードを変更する。

※インターネット上の各種サービスでは、多要素認証の利用を推奨

日頃から注意すべきセキュリティ対策ポイント⑧

アクセス制御・認可

- オフィスネットワークやクラウドサービスへの接続は、システム・セキュリティ管理者が指定した方法とし、**許可なく設定等を変更しない**。
- 業務端末において、**業務上必要のない無線機能（例：Bluetooth機能、アドホックモード等）は無効化**する。
- 複数人でデータを共有可能な場所（オフィスネットワーク上の共有フォルダ、ファイル共有サービス等）に機密情報を保存する場合、**情報を閲覧・編集する権限が誰にあるか確認し、適切な設定を実施**（テレワーク勤務者で設定できない場合はシステム・セキュリティ管理者に相談）する。
- オンライン会議にアクセスするための**URLを正規の参加者以外に公開せず**、出席者の確認をするなどして、第三者が会議に参加することのないようにする。また、**会議参加時のパスワード設定や**、待機室機能が有効化できる場合には、可能な限り設定する。

日頃から注意すべきセキュリティ対策ポイント⑨

インシデント対応・ログ管理

- セキュリティインシデントの発生に備えて、**連絡先と対応手順をあらかじめ確認しておく。**業務端末が操作不能になったり、サーバ障害でWeb参照が不可になることも考えられることから、連絡先は**電話番号等も確認**するようにしておく。
- 業務端末の紛失やマルウェア感染等のセキュリティインシデントが発生した場合（発生のおそれがある場合を含む）定められた連絡先へ速やかに報告する。動作が不審であるなど、**セキュリティインシデントかどうかわからない場合も速やかに報告**する。

※インシデント発生時における緊急連絡先を事前確認

日頃から注意すべきセキュリティ対策ポイント⑩

物理的セキュリティ

- **操作画面の自動ロック設定**や**プライバシーフィルターの貼付**等を行うほか、周囲にいる組織外の人の挙動に注意を払う。自宅等で家族がいる場合についても、不注意により意図せず情報漏えい等が起きる可能性があるため注意する。
- オンライン会議を実施するときは、**音漏れや画面を介した情報漏えい**が起きないよう注意する。オフィス内であっても、同じ場所で複数人が別のオンライン会議を実施等する場合の音漏れに注意する。

※常に業務を行う場所に気をつけなければならない

日頃から注意すべきセキュリティ対策ポイント⑪

教育

- セキュリティに関する研修等を受講し、**セキュリティに対する認識を高める**とともに、自らが実施している**セキュリティ対策状況**を確認する。
- 業務時に使用するツールの操作に習熟していないことにより、誤って情報を漏えいするリスクが懸念される
- オンラインコミュニケーションツールが提供するファイル共有、ファイルダウンロード機能に関するルールを定めておく

日頃から注意すべきセキュリティ対策ポイントまとめ

- 最新のアンチウイルス定義ファイルに更新
- OSやアプリケーションの最新セキュリティパッチを適用
- 会社から許可された手段でのみネットワークに接続
- 会社が定めたWi-Fi利用時の注意点の順守
- 強固なパスワード設定、多要素認証の導入
- 会社から許可されたクラウドシステムを利用
- クラウドシステムを利用する場合のルールの順守
- 社外での作業環境に注意
- 不審なメールに注意
- 持ち出した書類、USBメモリ等の取扱いに注意
- 定期的にセキュリティに教育を実施
- インシデント発生時における緊急連絡先を定めておく

本日の講義はここまでです
ご清聴ありがとうございました