2026年1月24日

標的型攻撃メールにご注意

「上司になりすますメール」「QR詐欺メール」が急増

株式会社　タカ
博士（工学）福永隆文
情報処理安全確保支援士（登録ｾｷｭﾘﾃｨｽﾍﾟｼｬﾘｽﾄ）
熊本商工会議所　登録専門家（セキュリティ部門）

標的型攻撃メール

標的型攻撃メールとは、特定の組織（企業、官公庁、教育機関、民間団体等）を攻撃する詐欺メールです。

攻撃者が例えば求人への応募などでメールのやり取りを繰り返して求人担当者が信用しきってしまったときにウイルス付き添付ファイルを送付したり（やり取り型攻撃）、その会社がよく利用するサイトに罠を仕掛け、アクセスした従業員のパソコンにウイルスを感染させる（水飲み場型攻撃）、テレワーク用の接続機器（VPN装置）などの脆弱性を利用して不正に侵入し（不正アクセス）、機密データの窃取・破壊を行うなど手法は様々ですが、特定組織を標的とする詐欺メールです。

最近は特に社長・上司や社内外の権威者からの（時には緊急性を強調した）メールで社員の方を（慌てさせて）騙す手法も多くみられます。権威者への信頼、緊急性を利用する「人間の心理を突いた攻撃」と言えます。

大企業を狙う前段階として傘下にある子会社（サプライチェーンに属する会社）を標的とするケースも増えています。最終的な標的は大企業ですが、まずは傘下のセキュリティが弱い子会社が標的になります。

IPA発表「10大脅威2025」の多くに標的型攻撃メールが使われています

順位	「組織」向け脅威
1	ランサム攻撃による被害
2	サプライチェーンや委託先を狙った攻撃
3	システムの脆弱性を突いた攻撃
4	内部不正による情報漏えい等
5	機密情報等を狙った標的型攻撃
6	リモートワーク等の環境や仕組みを狙った攻撃
7	地政学的リスクに起因するサイバー攻撃
8	分散型サービス妨害攻撃（DDoS攻撃）
9	ビジネスメール詐欺
10	不注意による情報漏えい等

メールの添付ファイルからウイルスに感染させたり、メール本文中にウイルスを仕込んだWeb サイトへのリンクを仕込み、感染させ、情報を窃取・暗号化し金銭を要求します。

商品の企画、開発から、調達、製造、在庫管理、物流、販売までの一連のプロセスに関わる全ての企業群をサプライチェーンと呼びます。その中でセキュリティが弱い企業に攻撃メールを仕掛け、最終的に親会社をターゲットにします。

機密情報を持つ組織に、攻撃メールを送り、機密情報を窃取します。事例ではJAXAや大手企業が挙げられています。

攻撃者が経営層や取引先になりすまし、従業員を騙して金銭の振込や機密情報の引き渡しをさせる巧妙な詐欺メール

詐欺メールの特徴

AIを使って自然な攻撃メールが作られるといっても注意すれば怪しい点はあるものです。

「@outlook.com」、「@outlook.jp」、「@hotmail.com」などのフリーメール使用は怪しい。

[SPAM]【PayPay銀行】送金失敗通知

返信　全員に返

<PayPay銀行> <japannetbank@uamlied.cn>
宛先　fukunaga@ict-taka.jp

このメッセージをテキスト形式に変換しました。

メールアドレスの末尾の国コードが自社に関係ない国コード（例：cnは中国）になっている

※PayPay 銀行

不自然

こんにちは、お客様の口座が異常のため、お客様の口座に振り込む際に、入金することが完了できません。。

ミス？

ご振込み金額は一応こちらで預かりますので、下記リンクから制限を解除してください。

ご本人確認の上、paypay 銀行から送金頂きます。

メールでの金銭要求はまず疑う

ファイル名の最後のドット（.）に続く拡張子がphp（プログラム）になっている。

▽お手続きはこちら

https://paypay-bank.hjvter.cn?wctxNBCW2101.doa.php

※メールを受け取ったお客さま専用のページです。ほかのお客さまはご利用いただけません。

--- 不自然 ----------

心配はいりません。スタッフが確認した後、お客様のアカウントに送金いたします。

これには時間がかかる場合があります。お手数をおかけして申し訳ありません。

不自然に複雑で怪しい。セキュリティソフトの検知を逃れるため不正URLには複雑なものが多く見受けられます。

「top、icu、co、shop」は詐欺メールのトップレベルドメイン（メールの一番最後）としてよく使われます。（無料で利用可）

インターネット再配達依頼 <https://toivipyamatojp.top/?6it2ids7>

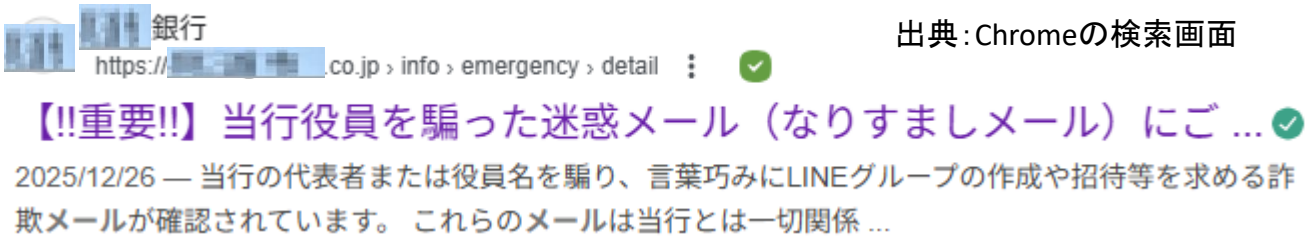
最近のメールによる攻撃事例

事例1:「LINEのグループを作成して」と社長を装ったメール詐欺

2025年12月から実在の経営者や役員の名前をかたり、「業務指示」を装って社員にLINEグループを作成させ、自身を招待させ、LINE内で社員に取引先口座（攻撃者の口座）にお金を振り込むように指示をする詐欺が急増しています。

警視庁、新聞、銀行から次々に警告が発せられています。

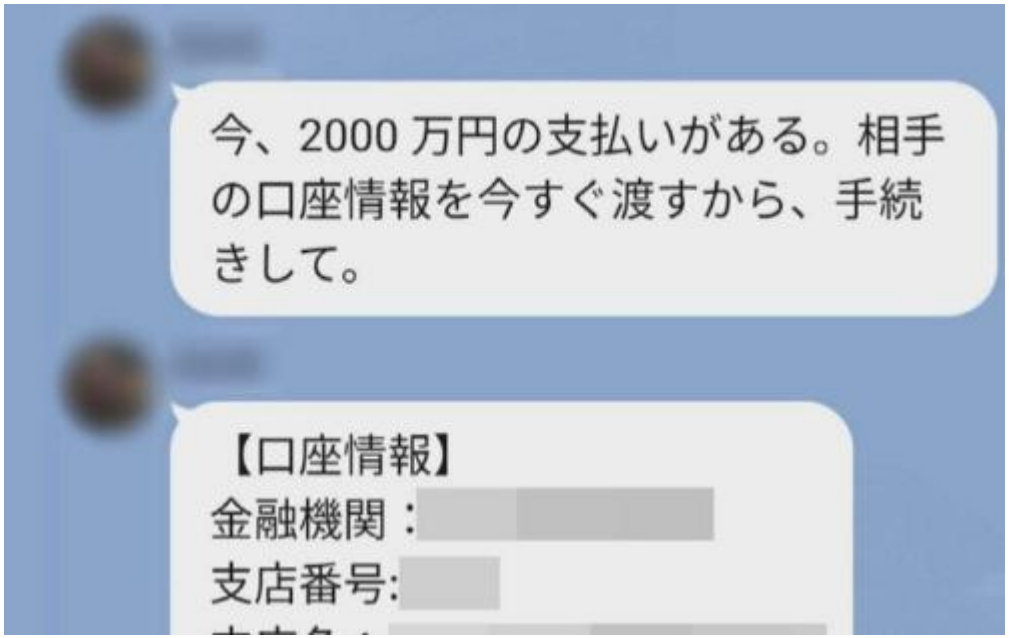
出典:Chromeの検索画面



「社長」を装った攻撃者からのメールの事例

出典：テレ朝NEWS https://news.tv-asahi.co.jp/news_society/articles/photos/900181591.html

LINEのグループを作成するとその中で振り込みを指示します

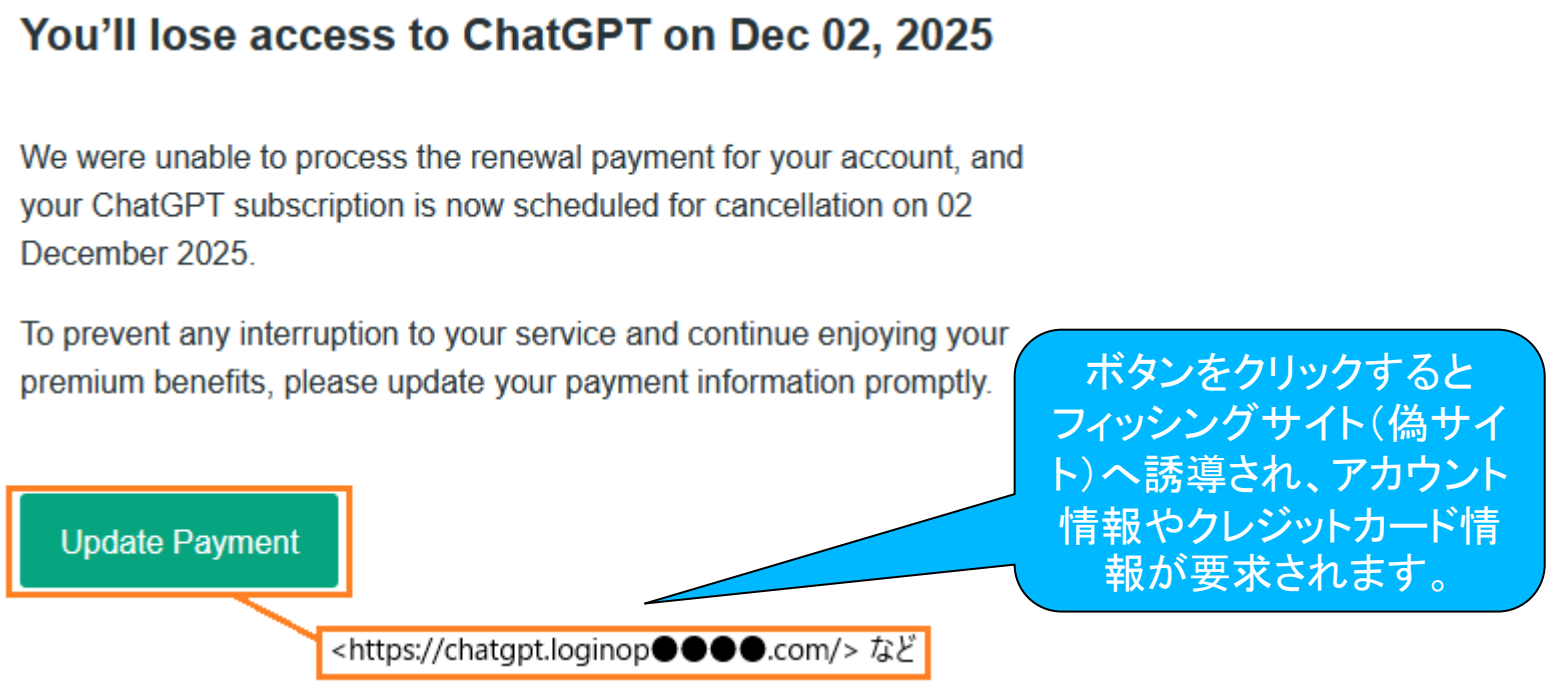


出典：https://news.yahoo.co.jp/articles/7e59e323ccf8f465d1b38da2f636f6997ce9e314/images/000

東京では4社あわせて1億4000万円の被害が発生しているそうです。

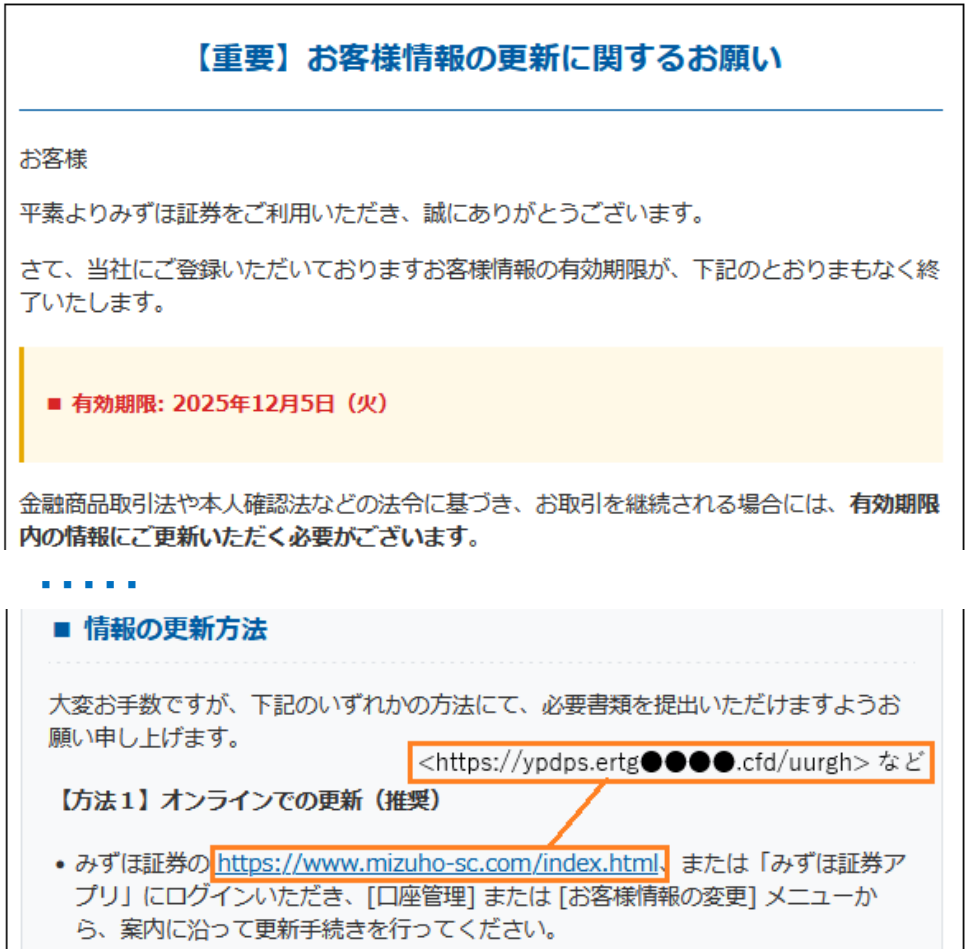
事例2： OpenAI (ChatGPT) をかたるフィッシングサイトへの誘導メール

実際の事例は英語ですが、今後、日本語版が発生する可能性もあります。



出典：フィッシング対策協議会：https://www.antiphishing.jp/news/alert/openai_chatgpt_20251202.html

事例3： 証券会社を装った詐欺メール



【重要】お客様情報の更新に関するお願い

お客様

平素よりみずほ証券をご利用いただき、誠にありがとうございます。

さて、当社にご登録いただいておりますお客様情報の有効期限が、下記のとおりまもなく終了いたします。

■ 有効期限: 2025年12月5日（火）

金融商品取引法や本人確認法などの法令に基づき、お取引を継続される場合には、**有効期限内の情報にご更新いただく必要がございます。**

・・・・・

■ 情報の更新方法

大変お手数ですが、下記のいずれかの方法にて、必要書類を提出いただけますようお願い申し上げます。

<https://ypdps.ertg●●●●.cfd/uurgh> など

【方法１】オンラインでの更新（推奨）

- みずほ証券の https://www.mizuho-sc.com/index.html、または「みずほ証券アプリ」にログインいただき、[口座管理] または [お客様情報の変更] メニューから、案内に沿って更新手続きを行ってください。

リンクをクリックするとフィッシングサイト（偽サイト）に誘導されます。

出典：フィッシング対策協議会：https://www.antiphishing.jp/news/alert/mizuhosc_20251204.html

対策

金銭要求するメール内のリンクはクリックしないようにしましょう。必要性を感じたら通常利用している（ブックマーク登録している）Webページ、または専用アプリからログインして確認しましょう。

金融機関、証券会社などでは専用アプリ、もしくはブックマークからサイトにアクセスして各種処理を行うことを推奨しています。

セキュリティ対策として、ネット倶楽部等の当社サービスを利用する際は、ブックマーク（お気に入り）からアクセスいただくことをお薦めします。みずほ証券の公式URLは以下のとおりです。

- みずほ証券ウェブサイト：**https://www.mizuho-sc.com/index.html**
- みずほ証券ネット倶楽部：**https://mnc.mizuho-sc.com/web/rmfIndexWebAction.do**

出典：みずほ証券　https://www.mizuho-sc.com/security/crime/phishing.html

・お勧めの対策
個人のお客さまは京銀アプリをご利用ください。ブラウザをご利用される場合は「お気に入り（ブックマーク）」からログインしてください。（出典：京都銀行ホームページ）

セキュリティソフトのフィッシングサイト対策はデフォルトで有効ですが注意は必要です

詳細設定 > 保護 > Webアクセス保護

表示例：ESET Internet Security V18.0

（注意）フィッシングサイトは日々更新されますので、すべてのフィッシングサイトがブロックされるわけではありません。
先にフィッシングサイトとして登録されている場合にはブロックしますが、新たなフィッシングサイトはブロックできません。

新たな攻撃手法：クイッシング詐欺（QR詐欺） QRコードに要注意

クイッシングは、QRコードを悪用したフィッシング詐欺（QR詐欺）です。現在はいろんな場所、広告にQRコードが利用されています。攻撃者は偽りのQRコードを張り付け、偽りの（本物そっくりの）Webサイトに利用者を誘導し、金銭や個人情報を盗みます。家賃の支払い、コインパーキング精算機、駐車違反罰金支払いの被害報告もあるそうで、広い範囲で悪用されています。

攻撃メールにもQRコードが利用されるケースが増えてきました。メール本文、PDFや画像の添付ファイルに不正なQRコードを張り付け、偽りのWebサイトに利用者を誘導し、金融情報や個人情報を盗みます。

メール本文のURL詐欺リンクはサービスプロバイダやセキュリティソフトが悪質URLデータベースにて検知できる可能性があります。しかし、QRコードの場合は従来の方法では検知ができません。

また、QRコードスキャンは多くの場合、スマホで行います。スマホのセキュリティ対策はPCと比べると貧弱な場合があるため、攻撃を受けやすくなってしまいます。

メール本文に詐欺QRコードが埋め込まれた事例

出典：フィッシング対策協議会　https://www.antiphishing.jp/news/alert/qr_20240828.html

ご利用明細のお知らせ

客様

平素よりお世話になっております。
【三井住友カード】でございます。

ご利用日時：2024年08月27日 10:58
ご利用場所：ビックカメラ（通販・ネットショッピングを含む）
ご利用金額：90,919円

この度、客様のカードご利用明細をご確認いただきたくご連絡申し上げます。

以下のQRコードをスキャンして使用詳細を取得してください。

クリックしてしまうと

アカウント情報、カード情報が盗まれてしまいます。

□の部分のリンク
<https://agre●●●●.top/>など

フィッシングサイト（偽サイト）

手の込んだ事例：PayPayを装ったQR詐欺メール

QRコードを悪用した詐欺メールが過去3年間で10倍に急増
（出典：2025年7月20日付の日経新聞）

QR詐欺、3年で10倍　PayPayは注意喚起
メールに添付→偽サイトに誘導　URLより判別困難
2025年7月20日 2:00 [会員限定記事]

新聞などで取り上げられたPayPayからの偽メールの被害の事例は下記の流れです。

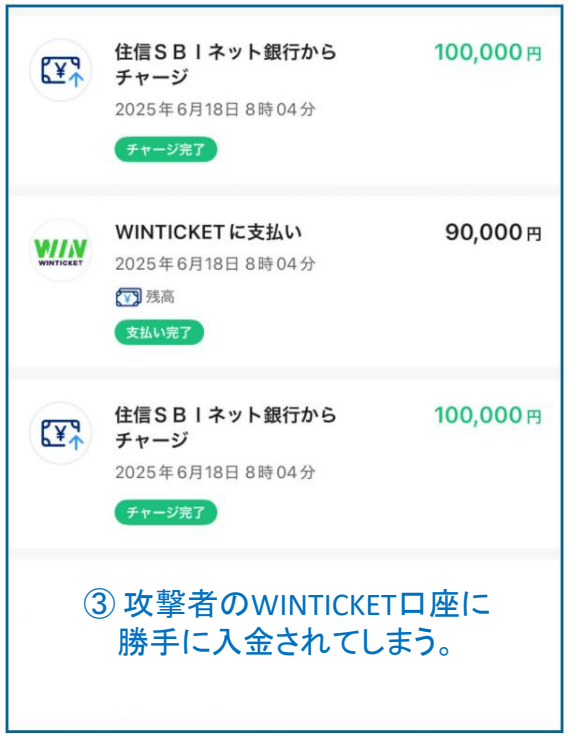
PayPayを装ったお知らせメール

①「アプリで請求明細を確認する」ボタンをクリックすると

（開いたサイトの画像：ぼかしをかけていますが、念のためQRコードは読み込まないように注意してください。）

② QRコードが表示され、促されるままにPayPayアプリでスキャンすると

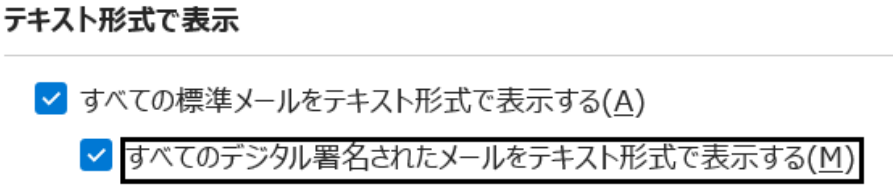
画像出典：
https://note.com/appliss/n/n419dcf130240



③ 攻撃者のWINTICKET口座に勝手に入金されてしまう。

対策

- 本対策に限らずメール本文はHTML表示をOFFにすべきです。仕事ではテキスト本文と添付ファイルがあれば十分なはずです。メールにブラウザと同じグラフィカルな表示を求めることは攻撃を容易にしてしまいます。



outlookではトラストセンターの設定で「テキスト表示」にします。

- QRコード添付によるメール攻撃が増えていますので、添付ファイル内のQRコードのスキャンは行わず（ブックマークの）信頼できるURLから、またはサイト専用のアプリがあれば、そちらから処理を行いましょう。

- QRコードを用いていろんな処理が実行できてしまうアプリの使用時は銀行口座との連携を解除する方が安全と思います（不便ですが）。併せて、そのアプリの安全性（セキュリティレベル）を注意深く調べることも必要です。

標的型攻撃メールを見分けるヒント

1. 件名、本文に書いてあることが身に覚えがない。
2. 件名、本文が金銭に関することで、しかも急がせる書き方である。
   例：「支払い方法を確認できず、注文を出荷できません.」
   「24時間以内にご確認がない場合、お客様の安全の為、アカウントの利用制限をさせていただきます」
3. 業務上の指示であるが、いつもと違う、違和感を感じる。
4. URLリンクに不自然に複雑な文字列がある。（※１）
5. 送信者のメールアドレスがいつもと違う。アドレス横のユーザ名表記がいつもと違う。
6. フリーメールアドレスを使っている。
7. メールアドレスの最後のトップレベルドメイン名が「top、icu、co、shop」などの見慣れないドメイン名である。（※２）
8. 送信時間が真夜中（不自然）である。
9. メール内リンクからパスワード入力画面へ遷移する。

   （必要があれば専用アプリ、ブラウザのブックマークからログイン）

（※1）迷惑メール全般に言えることですが、詐欺リンクには（セキュリティ検知回避のため）長い複雑な文字列が含まれることが多いです。通常のHTML表示のメーラーではこの複雑な文字列は隠ぺい可能です。
「テキスト表示」ではリンクの文字列が見えますので怪しい文字列に気付くことができます。
下記は例です。

（※2）
企業で国内取引のみの場合はメールアドレスの最後の部分は（例外もありますが）下記のいずれかです。（安全なドメインという意味ではありません）
.jp　.com　.org　.net　（まれに）.online

それ以外のアドレスはあまり使わないはずですので注意が必要です。たくさんありますが、例えば下記は国内業務を行う企業では使わないはずです。
.cn（中国）　.hk（香港）　.info（情報発信系サイト）　.pw（パラオ共和国）　.top　.xyz
icu（I see youの俗語）、co（コロンビア）、shop

番外編:画像検索にも注意

画像検索はクリックする部分にURL表示もなく、興味がある画像が表示されているため無造作にクリックされていませんか？

画像下の説明にポインタを合わせたときに表示される、左下のURLを確認し怪しいドメイン名になっていないかの確認は必要です。例えば、有名サイトのURLに酷似している、複雑な文字列が含まれているなどです。検索エンジン、ブラウザも対策はしていますが、最終的には自分の責任です。

出典:Chromeの検索結果画面より

日頃から少しづつ取り組むことが大きな防御力に

1. 仮に攻撃を受けた場合を想定した訓練を定期的に実施する。（標的型攻撃メール訓練など）
2. 情報リテラシー、モラルを向上させる。（セキュリティハンドブック、勉強会など）
3. 不審なメールは社内で相談・連絡し、情報共有する。一人の「気づき」を全社の「気づき」につなげる。
   標的型攻撃と思われるメールを発見したら情報管理者へ連絡をお願いします。
4. 関係者やセキュリティ業者、専門家と迅速に連携する対応方法や連絡方法を整備する。（緊急連絡網など）

セキュリティソフトにばかり頼らず、
自助努力がやはり必要です