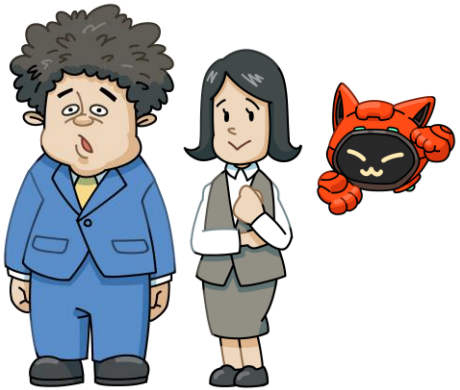
必ず身につけておきたいリテラシー

セキュリティ 7つの習慣 20の事例

セキュリティ教育資料



セキュリティ教育資料について

昨今、企業を取り巻くサイバーリスクが高まっており、セキュリティ教育の重要性がより一層強く求められています。
一方でセキュリティ教育にコストやリソースが十分にかけられない、セキュリティは専門用語が多く理解しづらい・難しくなりがちで、社員への理解浸透に課題を抱える企業も多いのではないでしょうか。
セキュリティ教育の目的は、一人ひとりにセキュリティを身につけてもらうことです。
そのためにはセキュリティを“自分ごと化”してもらうことが大切だと考えています。

MOTEXが提供するセキュリティ教育コンテンツは、教育資料・テスト・ポスターを通じて、今まで難しくて理解しづらかったセキュリティをわかりやすく伝え、従業員のみなさまへのセキュリティリテラシー向上を促すことができます。
サイバーセキュリティハンドブックと本資料を活用し「7つの習慣」を学んだ後、Q＆A形式の「20の事例」を解いていくことで、セキュリティに必要な基礎知識を身につけることができるようになっています。

セキュリティブック、本資料が皆様のお役に立てれば幸いです。

2026年2月
エムオーテックス株式会社

ご利用にあたって

---------- 資料を使用する前に必ずお読みください　----------

本資料はエムオーテックス株式会社（以下、当社）が提供する、
サイバーセキュリティハンドブック『セキュリティ 7つの習慣・20の事例』をもとにしたセキュリティ教育資料です。
セキュリティ教育や研修後の復習、理解度確認を目的として、無償にて提供しております。

【ご利用にあたって】
本資料の内容は、利用規約の範囲内において、自由に編集（変更・追加・削除）いただけます。
本資料の編集、複製、または内部利用（配信・実施等）を開始した時点で、規約全文に同意したものとみなされます。
ご利用前に、必ず規約をご確認ください。

＜コンテンツ利用規約＞　https://www.motex.co.jp/nomore/cybersecurityhandbook_policy.pdf

目次

はじめに

ITの進歩により便利になる一方、その影に潜むセキュリティリスクは他人事ではなく、あなたのすぐそばまで迫っています。

でも、セキュリティって専門用語が多くて難しそうだし、どう学べばいいかわからない。そう思っていませんか？

MOTEXが提供するサイバーセキュリティハンドブックは、今の時代に誰もが身につけておくべき「セキュリティ 7つの習慣」と、
その習慣をクイズ形式で学べる「20の事例」にまとめたものです。

セキュリティの基礎を学びたい方や、社会人としての教養を身につけたい方はぜひご覧ください。

登場人物紹介

BANNYA（バンニャ）

2050年からやってきたセキュリティ
知識が豊富な猫型ロボット。
未来を守るため、現代の人々にセキュ
リティ意識を広めるのが使命。

茂礼手 太郎
（もれて たろう）

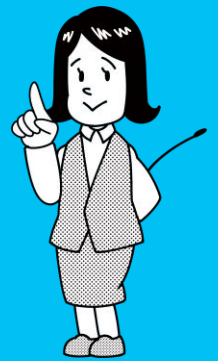
営業部の課長。
何かとトラブルに遭っては、
布施木さんに助けられている。
お調子者で、うっかり情報を漏らし
がち。

布施木　ます子
（ふせぎ　ますこ）

真面目で丁寧な仕事ぶりで、
なんだかんだ茂礼手課長をサポート。
しっかり者だから、これまで大きな
トラブルもなくやってきたけれど…

あなたの身近に潜む

セキュリティリスク



情報セキュリティ10大脅威 2026

「自分は大丈夫」という油断が最大の隙になります。
日常化するサイバー攻撃や新たな脅威から、自分や会社を守れるのは、一人ひとりの防衛意識です。

個人	順位	組織
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	ランサム攻撃による被害
インターネット上のサービスへの不正ログイン	2位	サプライチェーンや委託先を狙った攻撃
インターネットバンキングの不正利用	3位	AIの利用をめぐるサイバーリスク
クレジットカード情報の不正利用	4位	システムの脆弱性を悪用した攻撃
サポート詐欺（偽警告）による金銭被害	5位	機密情報を狙った標的型攻撃
スマホ決済の不正利用	6位	地政学的リスクに起因するサイバー攻撃（情報戦を含む）
ネット上の誹謗・中傷・デマ	7位	内部不正による情報漏えい等
フィッシングによる個人情報等の詐取	8位	リモートワーク等の環境や仕組みを狙った攻撃
不正アプリによるスマートフォン利用者への被害	9位	DDoS攻撃（分散型サービス妨害攻撃）
メールやSNS等を使った脅迫・詐欺の手口による金銭要求	10位	ビジネスメール詐欺

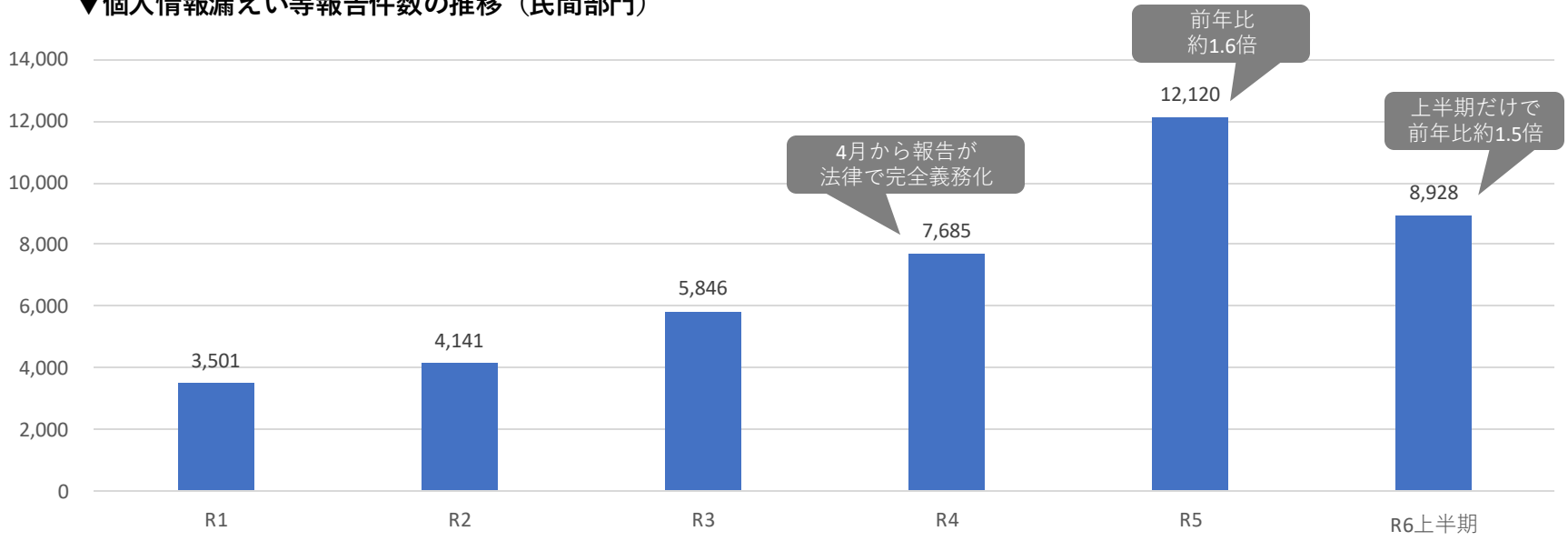
初選出

出典：「情報セキュリティ10大脅威 2026」（IPA：情報処理機構）
https://www.ipa.go.jp/security/10threats/10threats2026.html

セキュリティ事故（情報漏洩事故）について

「情報漏洩」はもはや特殊な事件ではありません。
業種・規模を問わず、日常的な経営リスクになっているのが現状です。

▼個人情報漏えい等報告件数の推移（民間部門）

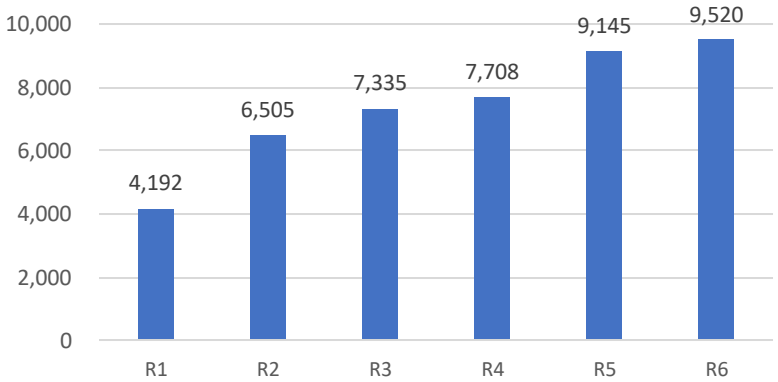


出典：個人情報保護委員会「年次報告」および「令和6年度上半期の活動状況について」より作成
https://www.ppc.go.jp/aboutus/report/

サイバー攻撃の情勢について

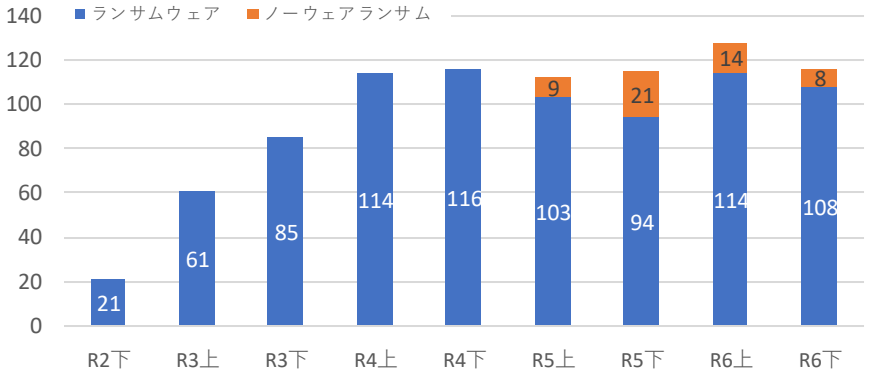
個人の端末やアカウントが、組織を標的としたサイバー攻撃の最初の「足場」にされます。
「常に狙われている」前提の防衛意識を持ちましょう。

▼サイバー攻撃件数の推移



2025年中、政府機関、交通機関、金融機関等の重要インフラ事業者等におけるDDoS 攻撃とみられる被害や情報窃取を目的としたサイバー攻撃、国家を背景とする暗号資産獲得を目的としたサイバー攻撃事案等が相次ぎ発生しています。

▼企業・団体におけるランサムウェア被害の報告件数推移



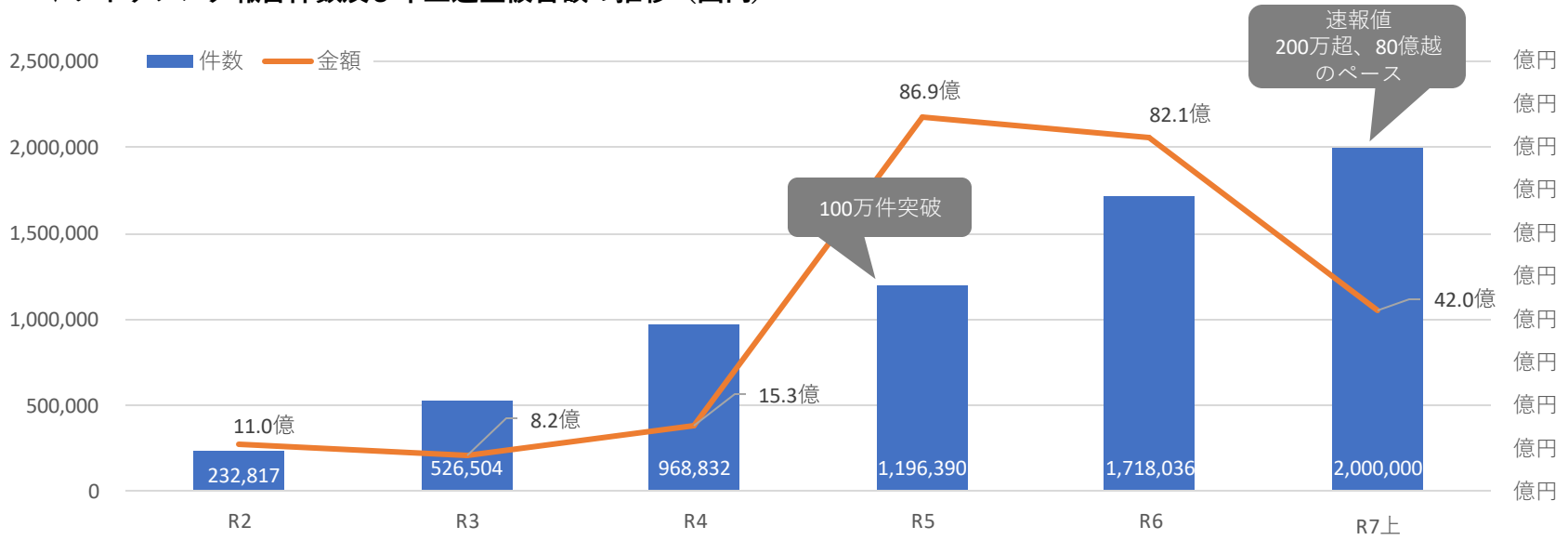
「ラムサムウェア」の被害報告件数も高水準で推移しています。

出典：警視庁「令和６年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/R6/R06_cyber_jousei.pdf

フィッシング詐欺について

AIによる巧妙な手口が、メールボックスに日常的に届く「回避不能なリスク」です。
「怪しいメール」は、もはや判別不能なのが現状・・・常に警戒心を持ちましょう。

▼フィッシング報告件数及び不正送金被害額の推移（国内）



出典：フィッシング対策協議会「月次報告書」をもとに作成
https://www.antiphishing.jp/report/monthly/

あなたの
デジタルライフを守る

7つの習慣

習慣 1 ｜ 誘導や催促のメッセージを警戒し、確認しよう

なんたって「人」がいちばんだまされやすい!!

最近の詐欺の手口は、驚くほど巧妙になっています。かつては「これは怪しいぞ」とすぐに見抜けたメッセージも、**今では本物と見分けがつかないほどそっくり**で、つい信じてしまうケースが増えています。
特に彼らが狙うのは、私たちの「焦り」や「不安」です。急ぎの対応を求めたり、不安をあおるような内容で、私たちから情報やお金をだまし取ろうとします。行政機関や金融機関、有名企業など、**多くの人が信頼する相手になりすましている**ため、疑うことなく焦って行動してしまうと、思わぬ被害に遭ってしまいます。

このような被害を防ぐためには、**「本当に正しいのか」と疑って立ち止まること**が大切です。

受け取ったメッセージには常に警戒心を持ちましょう。

ひと呼吸おく冷静さと、確認のひと手間が
最大の防御になるにゃ！

POINT 1 「フィッシング詐欺」や「なりすまし詐欺」に注意！

➢ **「フィッシング詐欺」**
銀行や通販サイト、宅配業者など、“誰もが知る有名企業やサービス”になりすまし、
不特定多数にメールやメッセージを送る手口。
「アカウント凍結」「再配達」といった緊急の連絡を装い、偽サイトへ誘導してIDやパスワード、
クレジットカード情報などをだまし取ろうとします。

➢ **「なりすまし詐欺」**
家族や友人、上司、取引先、行政機関など、あなたが“信頼している特定の相手”になりすまして接触する手口。
信頼関係を悪用し、不正な送金や情報の提供を直接指示・誘導してきます。

どちらの手口も、本物そっくりに装っているため、見分けるのが非常に難しいのが特徴です。

POINT 2 より巧妙化する「標的型攻撃」に注意！

➢ **「標的型攻撃」**
不特定多数ではなく、特定の個人や組織をターゲットにする、非常に悪質な手口。

例：取引先や社内外の関係者を装い、請求書や資料共有、人事通知などごく自然な内容のメッセージ

被害
ウイルス感染、情報漏洩やアカウント乗っ取り、さらに端末が「攻撃の踏み台」にされ、
会社や無関係な第三者にまで被害を広げる加害者になる恐れがあります。

✓ **内容だけでなく「送信元が誰か」を念入りに確認する習慣を身につける**
✓ **メールアドレスやURLが公式か所属や名前に違和感がないかを必ずチェック**

POINT 3 「今すぐ！」と言われてもひと呼吸おこう

➢ **「サポート詐欺」**

「ウイルスに感染しました」「今すぐサポートに連絡を」といった偽の警告をWebサイト上で表示し、
「緊急性」や「罰則」を装って利用者を動揺させ、考えるスキを与えない心理トリック。

被害

偽のサポート窓口に誘導され、その結果、攻撃者にあなたのPCをリモートで操作され、
個人情報が抜き取られたり、オンラインバンキングで多額の金銭を送金させられるなど。

- ✓ **冷静に状況を疑うこと**
- ✓ **たいていの場合、再起動やブラウザの強制終了で復旧します**
- ✓ **画面に表示されている電話番号には絶対連絡をしない**
- ✓ **対応が難しい場合は、情報システム担当者または警察に連絡**

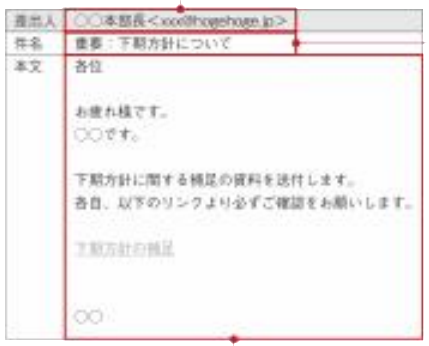
いますぐ実践！詐欺メッセージを見分けるには？

フィッシング詐欺やなりすまし詐欺の被害を防ぐために、
まず大切なのは「届いたメッセージを疑う」習慣を持つことです。
最近の詐欺メッセージは、デザインや文面が本物そっくりで、気づかないうちに
リンクや添付ファイルをクリックしてしまうケースが増えています。

要チェック いますぐ使えるチェックポイント

- ✓ リンクを安易にクリックしない
- ✓ 広告や見慣れないサイトへのリンクに注意
- ✓ 送信元を確認する
  - ・ドメイン名が正規の表記か（例：example.com）
  - ・よく見るとスペルが違う
  - ・数字や記号が混ざっている
  - ・差出人名は正しそうでも、アドレスが公式と異なる
- ✓ 個人情報提供の要求には応じない
- ✓ 迷ったら公式サイトから確認する

超重要 メールの安全性を確認する方法



① 差出人メールアドレス

差出人の表示名とアドレスがまぎらわしい組み合わせか、仮に差出人に心当たりがあっても、ドメイン名の文字列をよく確認しましょう。少しでも不安がある場合は、送信者に電話や別の手段で確認をとりましょう。

②メールの件名

攻撃メールは、受信者に興味させるため、「内容確認の依頼」となっていることが多いです。実際、「先日の打ち合わせについて」や「至急の確認依頼」といった業務と心当たりがありそうな表現になっています。件名だけ読むと中身を確認する必要があると思い込みがちですが、「①差出人メールアドレス」とセットで確認する習慣をつけましょう。

③添付ファイルやメール本文に設置されたリンク

添付ファイルについては、「拡張子とアイコンが合っていないファイル」「二重拡張子のファイル」「実行形式の拡張子のファイル（例：.exeなど）」になっていないか確認しましょう。本文中のリンクについては、マウスオーバーをすると「アクセス先のURL」を表示できる機能などがあります。URLのドメイン名の文字列を確認し、不審なURLであればクリックしないようにしましょう。

その内容、ネットに発信しても大丈夫？

SNSが浸透し、インターネットへの情報発信は手軽で日常的になりましたが、その投稿には**個人や他人のリアルな情報がたくさん含まれていることが多く、そこに大きなリスク**が潜んでいます。
なにげない投稿から**行動パターンがバレたり**、位置情報や写真・動画から**自宅や職場が特定**され、ストーカーや空き巣の被害につながります。また、仕事や会社の情報をうっかり投稿したことで**機密情報が漏れ**、悪用されるといったケースも発生しています。
特に最近は、攻撃者がターゲット企業の従業員のSNSを調べて情報を集めるケースが確認されており、あなたの投稿は攻撃の準備段階における有力な情報収集手段となり得るのです。

一度ネットに公開された情報は、**「デジタルタトゥー」**として半永久的にインターネット上に残り続けます。投稿した瞬間はよくても、将来的にあなたに不利益をもたらす可能性があるため、**少しでも誰かに知られたら困る情報は、絶対に発信しない**こと。
プライバシーと機密保持の意識を高く持ち、
慎重な情報発信を心がけましょう。

投稿前には必ず一度立ち止まって、「誰かに見られたらどうなる？」
「仕事に影響しないか？」考えてみることだにゃ！

POINT 1 なにげない投稿が招く「個人特定」に注意！

SNSの投稿の中に、個人情報やプライバシーに関わるものが含まれていませんか？

リスク 行動範囲や居場所が特定される可能性

- ✓ **位置情報がオンになっていないか**
- ✓ **自分以外の他人や家族が写っているもの、タグ付けも要注意**
- ✓ **プライバシーへの配慮**

POINT 2 仕事や職場に関する情報は「機密」と心得よう

仕事や職場に関する投稿には、特に細心の注意を払いましょう。
断片的な情報でも、つなぎ合わされ、会社の動向が筒つけになってしまうこともあります。

リスク

・出張先や新製品の写真をアップしてしまうと、業務上の機密情報が漏れる可能性
・内輪の話や不満をSNSでつぶやいたことで、職場や組織のイメージダウン
・無意識のうちに社外秘の情報をさらしてしまう可能性

- ✓ **仕事や職場に関する情報は、「もしかしたら機密情報かもしれない」と常に意識する**

POINT 3 「デジタルタトゥー」になり得ることを意識しよう

➢ **「デジタルタトゥー」**
一度インターネット上に公開した情報は、タトゥー（入れ墨）のように半永久的にネットに残り続けます。

リスク

・あなたが不適切な発言や写真・動画をSNSにアップし炎上してしまった場合、
あっという間に拡散され、あなたの名前を検索すると、何年経っても過去の炎上情報が表示される
・カッとなった勢いやその場のノリで投稿した内容は、さまざまな価値観を持つ不特定多数の人が
集まるインターネット上では、後になって大きな問題になってしまうこともある

✓ **発信する前には一度冷静になって、「本当にこの内容で大丈夫かな？」と投稿を見直すこと**

POINT 4 公開範囲とアカウント連携に注意しよう

SNSを使うときは、「誰に自分の情報を見せるか」という設定（公開範囲）を必ず確認し、
「友達だけに公開」など、閲覧者を限定的にする設定を活用しましょう。

リスク

・非公開アカウントでも、他サービスとの連携で投稿が表示されることも
・非公開アカウントの内容を公開の場に転載して炎上

✓ **複数のSNSアカウントを連携するときは、連携先サービスのプライバシー設定も忘れずに
チェックし、必要な設定に変更**

習慣 3 パスワード管理アプリと多要素認証を使いこなそう

パスワード管理はセキュリティの基本の「き」!!

あなたの**IDとパスワードは、「私が本人です」と証明するための、とても大切な情報**です。これは、自宅や会社の入口の鍵にも匹敵する、デジタル環境におけるセキュリティの要（かなめ）と言えます。
もしパスワードが盗まれたら、単にアカウントの情報が漏洩するだけでは終わりません。
個人の場合は、オンラインバンキングの不正利用やクレジットカードの悪用といった金銭的被害に加え、流出した情報が悪用されて新たな犯罪や詐欺の踏み台にされる恐れがあります。企業や組織の場合は、システムダウンによる事業停止や、会社の機密情報・顧客情報の漏洩による社会的信用の失墜など、取り返しのつかない事態に発展してしまうこともあります。

パスワードは、**簡単に推測されないように、十分に長くするのが基本**です。しかし、サービスごとに異なるパスワードを作り、それらをすべて覚えておくのは現実的ではありません。そこで活用すべきなのが、**「パスワード管理アプリ（パスワードマネージャー）」**です。
パスワード管理アプリを使った安全なパスワード管理の方法を身につけましょう。

ウソのような本当の話…世界的に最も多く使われているパスワードの上位は「123456」や「password」、「asdfghjkl（キーボード順）」なんだにゃ。
あなたは大丈夫？

POINT 1　パスワード管理アプリ（パスワードマネージャー）を活用しよう

パスワード管理で最も危険なのは、**「推測されやすいパスワード」**と**「使い回し」**です。

リスク　パスワードを複数のサイトで使い回していると、一つ破られただけで芋づる式にすべてのアカウントが危険にさらされます。

- ✓ **推測されやすい、誕生日やペットの名前など好きな単語をパスワードにすることを避ける**
- ✓ **パスワード管理アプリなどで生成した十分に長い文字列にする**

POINT 2　顔認証や指紋認証を積極的に使おう

➢ **「生体認証（顔認証・指紋認証など）」**

顔認証や指紋認証は、顔を向けたり指を置くだけでログインができるので、非常に簡単で便利です。
しかも生体情報は一人ひとり異なるので、他人が手に入れたり真似することは困難で、
非常に高いセキュリティを保つことができます。

- ✓ **スマホやPCで生体認証が設定できるものは積極的に活用する**

習慣 4 OSやアプリを最新状態にアップデートしよう

最新の状態にしないとどうなる？

スマホやPC、アプリを動かすための「基本ソフト」であるOSは、**常に最新の状態を保ちましょう**。なぜなら、ソフトウェアには、開発段階で意図せず生じたセキュリティ上の欠陥、いわゆる「脆弱性」が潜んでいる可能性があるからです。

古いOSやアプリを使い続けていると、脆弱性が残ったままとなり、攻撃者にとって格好の「餌食」となります。**攻撃者は、この脆弱性を狙ってウイルスやランサムウェア（身代金要求型ウイルス）を仕掛けたり**、あなたの大切な情報を盗み出したりします。さらに、あなたのスマホやPCを使って会社のネットワークに不正アクセスするなど、さらなる攻撃の「踏み台」にされるリスクも高まります。

OSやアプリの提供会社は、こうした脆弱性を修正し、セキュリティを強化するための「アップデート」を常に提供しています。**アップデートの通知が来たら決して後回しにせず、速やかに対応しましょう**。これは、そのとき一番新しいセキュリティ対策が適用された状態で利用することが、何より大切だからです。

古いまま使い続けるのは、まるで「壊れた窓」から家に入れる状態を、泥棒に自ら差し出しているようなもの。放置しがちな更新…でも実はとても大事にゃ！

POINT 1 OS のアップデート通知が来たら「すぐ」が鉄則！

スマホやPCにOSアップデートの通知が届いたら、すぐに対応しましょう。
OSのアップデートは、システム全体のセキュリティを強化してくれるだけでなく、
新しい便利な機能の追加や、脆弱性の修正なども含まれています。

✓ **アップデートを後回しにしない**

POINT 2 使用するアプリを最新の状態に保とう

スマホやPCに入っている、普段あなたが使用しているアプリのアップデート通知も
見逃さないようにしましょう。

例：LINEのようなメッセージアプリ、Google Chrome・MicrosoftEdge・SafariといったWebブラウザ、地図アプリ、
SNS、通販サービス、オンラインバンキングなど

リスク

・古いバージョンを使い続けていると、脆弱性を突かれて危険なファイルを
ダウンロードさせられる可能性

✓ **アップデートを後回しにしない**

POINT 3 「自動アップデート」が断然おすすめ！

自動アップデートにしておけば、手動で対応する手間が省け、常に最新バージョンが使えて安心です。
うっかりアップデートを忘れてセキュリティ上の弱点（脆弱性）が放置されてしまうリスクも
防ぐことができ、使用頻度の低いアプリの対応漏れの心配もありません。

- ✓ **OSやアプリの自動アップデートが有効になっているかをチェック**
- ✓ **「Wi-Fi接続時のみ」にしておけば、通信費用を気にせず自動アップデートができる**

POINT 4 アプリは「公式」からダウンロードしよう

新しいアプリをダウンロードするときは、必ず公式のアプリストアや公式サイトから
入手するようにしましょう。＜スマホならGoogle PlayストアやApp Store、PCならサービス提供元の公式サイト＞

リスク

・偽物や詐欺目的のアプリが紛れ込んでいる可能性
・知らない間にスマホやPCが感染してしまう可能性

- ✓ **人気アプリにそっくりな偽物に注意**
- ✓ **アプリ名で検索しても、怪しいダウンロードサイトが上位表示されることも・・・**
- ✓ **提供元が公式であるかを確認する**

習慣 5 アプリやサービスは初期設定のまま使わず、設定を確認しよう

初期設定のままにしておくとどうなる？

現代の生活に欠かせない、さまざまなアプリやサービスは、私たちの生活をより便利にする一方で多くの情報を保持し、他のサービスと連携する機能も持っています。そのため、初期設定のまま使い続けていると、**あなたの情報が意図せず漏れてしまい、不正なアクセスやプライバシーの侵害につながるリスク**があります。

例えば、新しくインストールしたアプリのデフォルト設定が広範囲なアクセスを許可している場合、連絡先（アドレス帳）や位置情報、カメラ・マイク、ライブラリ（写真や動画のアルバム）、カレンダー、通話・メッセージなどから、**あなたや大切な人のプライベートな情報が外部に漏れてしまう**ことがあります。特に、アドレス帳と連携した機能により、友人・知人に同意を得ることなく、知らぬ間に彼らの連絡先を共有してしまうことがあるため、注意が必要です。

また、位置情報が漏れることで、ストーカーや空き巣被害の原因になることもあります。

新しいアプリを入れたら、**利用開始前に必ず、各項目を自分の目的にあった設定に変更**しましょう。

初期設定は、“あなたのため”を考えた、あなたに最適な設定になっているとは限らないにゃ！

POINT 1 初期設定は危険！最優先で「ログイン認証」を強化しよう

新しいアプリやサービスを使い始めるときには、まず「ログイン認証」の設定を必ず確認しましょう。

- ✓ **ログイン時の認証は、生体認証や多要素認証を積極的に活用**
- ✓ **初期パスワードが設定されいる場合は、必ず変更**
  （推測されにくく、十分に長い、他で使用していない強力なパスワードを）

POINT 2 アクセス権限と情報の公開範囲を見直そう

スマホやPCからさまざまな情報へのアクセスを求められたら、
その「アクセス権限」が本当に必要かを必ず見直しましょう。

- ✓ **アプリから要求されるアクセス権は、１つずつ確認し、不要なものは無効に**
- ✓ **プロフィールや連絡先などの個人情報の「公開範囲」も要確認**
  ※初期設定で公開となっている場合も多い

POINT 3 位置情報の設定は慎重に！

位置情報の共有は、本当に必要なときだけに絞ることが大切です。

- ✓ **本当に必要なアプリ以外は無効にするか「利用中のみ許可」設定にする**
- ✓ **機能上必須であるかのように見せて許可を求めてくるケースもあるので注意**
- ✓ **写真や投稿に位置情報が含まれたまま共有されることもあるので注意**

見えないところで組織を危険にさらしてしまう「シャドーIT」と「内部不正リスク」

無意識の行動でも危険を招く―シャドーIT

「シャドーIT」とは、企業のIT部門が把握・承認していない機器やアプリを、従業員が業務で使ってしまうことを指します。
「業務効率を上げたい」「少しなら大丈夫」という個人の判断は、会社のセキュリティ対策が及ばない場所でデータを扱うことになり、漏洩や不正アクセスのリスクが高まります。また、多くの企業では利用ルールを定めており、コンプライアンス違反に問われる可能性もあるため、十分な注意が必要です。

こんな行動、心当たりはありませんか？

- 個人アカウントの Google Drive／Dropbox に業務データをアップロード
- LINE・Messenger・WhatsApp など、会社で許可されていないアプリで業務連絡をしている
- Trello・Asana・Notion などの業務ツールを、IT部門に相談せず個人判断で使い始めている
- GigaFile便・WeTransfer など、ファイル共有サービスでデータのやり取りをしている
- 個人利用の生成AIツール（ChatGPT や Gemini など）に業務情報を入力している
- 私物のUSBメモリ・PC・スマホで業務データを扱っている

故意の行動が深刻な結果を招く― 内部不正

企業・組織にとって、外部からの攻撃だけでなく「内部の従業員による不正な行為」も重大な情報漏洩リスクとなります。こうした行為は総じて「内部不正」と呼ばれます。
内部不正とは、顧客データ、技術情報、企画や戦略、人事情報などの重要な情報を、故意に盗んだり、持ち出したり、破壊したりする行為を指します。「バレなければ大丈夫」「ちょっと魔が差しただけ」― そうした行動は、重大な不正行為となり、法的な責任を問われる場合があります。その結果は自分だけでなく、職場の仲間や家族にも影響が及ぶことを忘れてはいけません。

内部不正が招く「取り返しのつかない代償」

☑ 法的責任が問われる可能性
会社の機密情報（営業秘密）を不正に取得・使用・開示する行為は、不正競争防止法で禁じられています。このような行為は、内容によっては懲役や罰金などの刑事罰の対象となる場合があります。

☑ 損害賠償を求められる可能性
不正な持ち出しによって会社に損害が発生した場合、多額の賠償責任を負うケースもあります。個人への影響も小さくありません。

☑ 信用やキャリアへの影響
悪意ある情報持ち出しは懲戒処分の対象となり、退職・信用低下・転職への影響など、キャリアに大きなダメージを残す可能性があります。こうした影響は本人だけでなく、家族の生活や将来にも負担を与えてしまうことがあります。一度失った信用を取り戻すことは容易ではありません。

今こそスマホ・PCの重要性を考えよう

いまの時代、スマホやPCは私たちの暮らしや仕事に一日たりとも欠かせない存在となりました。
調べものや人とのコミュニケーション、趣味、仕事など、日常のあらゆる場面で端末を肌身離さず持ち歩いています。お財布や定期券から健康管理や自宅の鍵、家電のリモコン操作まで、**スマホ一つで生活のすべてが完結する**ほど、その利便性は増すばかりです。
しかし、こうして便利になればなるほど、**端末を紛失したり盗まれた場合の影響は非常に大きく**なります。
端末自体が高価なため転売目的で盗難に遭うこともありますが、**最も深刻なのは端末内の「情報」が悪用されてしまうこと**です。

あなたのスマホやPCは、端末の中に入っている**“情報を含めて”あなたの大切なデジタル資産**です。その重要性を再認識し、万が一のダメージを最小限に減らす対策をしましょう。

警視庁によると、１年間の携帯電話遺失届だけでなんと14万件※！ こんなにたくさんの端末が日々、持ち主の手元を離れているかと思うと、紛失・盗難は決して他人事ではないにゃ…

※参考：警視庁 遺失物取扱状況（令和6年中）

POINT 1 画面ロックは必須！あなたのスマホ・PC を守る「最初の扉」

画面ロックは必ず設定し、他の人が簡単に端末を開き、端末内の情報にアクセスできないようにしましょう。

- **「生体認証」**
  顔や指紋など、本人の生体情報を鍵として使う方法です。利便性が高く、なりすましが困難です。

- **「なりすまし詐欺」**
  パスワード・パスコード、PINコードは、本人しか知らない情報を鍵として使う方法です。
  設定する場合は、他人に推測されにくいものにしましょう。

POINT 2 万が一に備える！「探す」・「消す」の事前対策

万が一、スマホやPCを紛失したり盗まれてしまったときのために、事前の対策が非常に重要です。

✓ **端末の「位置情報サービス」と「検索機能」をオンにする**
iPhoneやMacなら「探す」機能。Androidなら「デバイスを探す」機能。Windows PCならMicrosoftアカウントのWebサイトから、位置情報を確認できる。

✓ **「リモートロック」と「データ消去」も設定**
端末が手元になくても、遠隔操作でロックをかけたり、保存されているデータをすべて消去できるので、紛失時に情報が悪意ある人の手に渡るリスクを大きく減らすことができる。

POINT 3 公共の場での「覗き見」と「情報漏洩」に注意！

公共の場でスマホやPCを使用するときは、次のことを意識しましょう。

- ✓ **端末は常に手元に置き、無防備に放置しない**
- ✓ **覗き見防止フィルムを貼る**
- ✓ **パスワードを入力するときは、周囲に人がいないかを確認、見えにくい角度で入力する**
- ✓ **不要なBluetoothやWi-Fi接続をオフにし、信頼できるネットワークのみを使用する**
- ✓ **重要な通知が画面に表示されないよう、ロック画面での通知設定やアプリの通知設定も見直す**

POINT 4 盗難対策の最優防御線として「暗号化」と「バックアップ」も忘れずに

- ✓ **容易に端末の中のデータを見られないようにするための「データ暗号化」**

  iPhone はパスコードや生体認証（Face ID ／ Touch ID）を設定することで、自動で暗号化が有効になります。
  Android デバイスの多くは初期設定で暗号化されてるが、念のため設定アプリの「セキュリティ」などで確認しておくと安心です。PC では、Windows なら「BitLocker」、Mac なら「FileVault」を使えば簡単に暗号化が有効にできます。

- ✓ **データを復旧できるようにするための「バックアップ」**

  システム設定にあるバックアップ機能を有効するか、GoogleDrive、iCloud、OneDriveなどのクラウドサービスを利用して、大切なデータのバックアップをこまめに取る。

「ショルダーハック」って？覗き見に注意！

「**ショルダーハック**」とは、あなたがスマホやPCを使っているときに、後ろや横から画面を覗き見して、パスワードや個人情報を盗み取る行為のことです。原始的な方法ですが、外で無防備に操作をしていると、情報漏洩につながります。公共の場でスマホやPCを使うときには、「覗かれているかもしれない」という前提で、しっかり対策をすることが大切です。

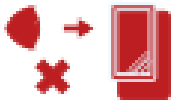
いますぐできる！ショルダーハック対策

物理的な対策

✓ **壁や柱を背にして座る**
背後からの視線を物理的に遮ることができるため、シンプルですが効果が高い方法です。

✓ **PCやスマホの画面を見せない**
画面が見える状態で放置しないようにしましょう。
不使用時はノートPCを閉じる、スマホカバーを付ける、また画面を下向きに置くことも有効です。

ツールによる対策



✓ **覗き見防止フィルムを貼る**
プライバシーフィルターやプライバシーフィルムは、特定の角度からしか画面が見えないように設計されているため、横からの視線をしっかり遮ることができます。

✓ **画面の明るさを落とす**
画面の明るさが自動調整される設定にしておくと、周囲から画面が見えにくくなります。

行動の工夫

✓ **公共の場での「重要情報の入力」に注意**
認証情報や個人情報、決済情報などは、入力前に周囲に人がいないかチェックし、手元や画面が見えにくい角度で操作しましょう。

✓ **周囲に不審な動きや近い距離に人がいないか気を配る**
突然近づいてきたり、手元を覗き込んでくるなどの不自然な動きをする人がいないか注意しましょう。覗き見だけでなく、スリなどの盗難対策にもなります。

習慣 7 少しでもおかしいと思ったら、すぐに相談しよう

「あれ？」と思ったら、すぐに相談！初動が大事！

最近のサイバー攻撃や詐欺はとても巧妙で、本物そっくりなメッセージが送られてくるため、**「これは怪しいぞ」と気づくこと自体がどんどん難しくなっています**。だからこそ、“ほんの少しでも違和感を覚えたら、すぐに誰かに相談する”という行動が非常に大切です。「こんな些細なことで相談していいのか」とためらうようなことでも構いません。
結果的に杞憂（きゆう）で終わってもよいのです。怖いのは本当に詐欺や攻撃に遭っていた場合で、
時間が経てば経つほど被害が拡大する可能性があるからです。

一人で抱え込まず、信頼できる人や専門窓口にすぐに相談することが、被害を防ぎ、もし被害に遭ってもダメージを最小限にするための最善策となります。日頃から**「何かいつもと違うな」と感じたらすぐに動く**、“初動”の習慣を身につけましょう。

会社でも、気づかずリンクをクリックしてしまったり、小さな違和感を覚えたら、ためらわずにすぐ上司や情報システム担当者に報告しよう！「怒られたらどうしよう…」と思わないで！ セキュリティも仕事と同じ、ホウレンソウ（報告・連絡・相談）が鉄則だにゃ！

POINT 1　不安を感じたら、警察相談ダイヤル「＃9110」へ！

✓ **一人で悩まず、「#9110（シャープ・イチ・イチ・マル）」へ相談**

このダイヤルは、犯罪や事故に当たるのか分からないけど警察に相談したいという場合に利用できます。
寄せられた相談には、内容に応じて警察の専門部署が連携し、具体的なアドバイスや指導、場合によっては相手方への警告、捜査や検挙といった、あなたの不安を解消するために必要な措置を講じてくれます。

✓ **実際に被害に遭ったり、緊急を要する事件や事故の場合は、迷わず「110番」へ電話**

すぐに連絡・相談が鉄則！！

所属組織での相談先を確認しておこう！

トラブルが起きたときにすぐ相談できるよう、会社や組織の情報システム担当者・セキュリティ担当者・CSIRT・サポート窓口・管理部門などの連絡先を書き留めておきましょう。

MEMO

困ったときの相談先

◉ IPA「情報セキュリティ安心相談窓口」（個人向け）
ウイルス感染、不正アクセス、迷惑メール、フィッシングなど、一般の利用者向けの情報セキュリティ相談に応じる窓口です。技術的なアドバイスを無料で受けられます。

◉ IPA「サイバーセキュリティ相談窓口」（企業向け）
企業や団体を対象とした、サイバー攻撃や情報漏洩などのセキュリティに関する相談窓口です。専門的な技術支援や必要な機関への案内を行います。

◉消費者庁「消費者ホットライン（188）」
☎188（局番なしで「いやや！」）※通話料金が発生します。（相談は無料です）
悪質商法、架空請求、ネット通販トラブル、フィッシング被害など、消費者トラブル全般の相談を受け付けています。お住まいの地域の消費生活センターにつながります。

◉ IPA「情報セキュリティ安心相談窓口」（個人向け）
実際に被害が発生した場合や、犯罪の疑いがある場合に相談できる窓口です。
全国の都道府県警察が対応しており、詐欺、SNS乗っ取り、ハッキングなどの通報が可能です。

あなたの
デジタルライフを守る

7つの習慣

01 よく見かける通販サービスからお得な特典情報が届いた

最近、通販サービスでの買い物にハマっている茂礼手課長。気になっていた通販サービスから「今だけ1万円分のポイントバック!!」というお得なメッセージが来て、リンクから会員登録に進むよう促されている。有名で魅力的なサービスだし、今だけ限定でお得な買い物ができそうなので、急いで会員登録をしようと思ったが…。

Q 下の選択肢から適切なものを選ぼう！

1. すぐにメッセージのリンクをクリックして、
   会員登録に必要な情報を入力する
2. 送信元のアドレスを確認し、
   問題なければリンクをクリックする
3. 公式サイトでそのキャンペーンが
   本当に開催されているのか確認する

01
A

3 公式サイトでそのキャンペーンが本当に開催されているのか確認する

特典や還付金といった“おいしい”話が突然届いても、メッセージ内のリンクをクリックしてはいけません。
攻撃者が個人情報や金銭をだまし取るための常套手口の一つで、「**フッシング詐欺**」の可能性があります。

解　説

リンクをクリックしてしまうと偽の銀行サイトやショッピングサイトに誘導され、個人情報や決済情報の入力を求められます。その結果、攻撃者に情報を盗まれ、クレジットカードの不正利用や銀行口座からの不正送金など、金銭的な被害に遭う危険があります。また、最近はアドレスも偽装されていることがあり、送信元の確認だけでは不十分です。

- ✓ **公式サイトや公式アプリを確認し、正しい情報かを確認する**
- ✓ **不安な場合は何もせずメッセージを削除する**

最近は、Web広告が悪用され、検索上位に表示されたサイトが実は偽サイトだったというケースも確認されているにゃ。
日常的に使うサイトは正しいURLをブックマークしておいたり、公式アプリを活用したりするのも有効な対策になるにゃ。

02 突然、大きな音とともに画面いっぱいにウイルス感染の警告が出た

茂礼手課長がWebサイトを見ていると突然、「ウイルスに感染しました」のポップアップが表示された。ポップアップには、修復用ソフトウェアのインストールを促す指示と、すぐに連絡するようサポート窓口の番号が記載されている。大きな警告音が鳴り止まないし、画面も固まってしまって操作できないし、ただならぬ事態なので、この番号に連絡してみようと思ったが…。

Q 下の選択肢から適切なものを選ぼう！

1. 画面の表示に従って、
ソフトウェアをインストールする

2. 画面の表示に従って、
記載されたサポート窓口に電話する

3. まずは「ESC」キーで
画面を閉じられるか試してみる

02
A

3

まずは「ESC」キーで画面を閉じられるか試してみる

突然の警告音やポップアップは「**サポート詐欺**」の典型的な手口です。
焦って画面の案内に従って連絡すると、個人情報や金銭をだまし取られる危険があります。

解　説

偽の警告を利用する「サポート詐欺」の手口には、このような「ウイルス感染」の警告のほか、「ライセンス切れ」や「アカウント不正利用」などの通知で不安をあおるケースもあります。さらに最近は、検索結果や広告から偽の窓口に誘導する手口や、「システム修復」や「遠隔サポート」を装ってツールをダウンロードさせ、ウイルスを仕込むケースも確認されています。

- ✓ **まずは「ESC（エスケープキー）」を長押しして全画面表示を解除、「×（閉じる）」ボタンで表示を閉じられるか試す**
- ✓ **閉じられない場合は、PCを強制終了し、再起動する**

ESCキー長押しで解決しない場合は、作業中のプログラムを終了させるショートカットキー（「Alt」+「F4」）や、タスクマネージャーを起動しブラウザを強制終了する方法（「Ctrl」+「Alt」+「Delete」）、それでもダメな場合にPCの再起動という方法があるにゃ。

03 上司からの急ぎの確認依頼メールが届いた

ます子さんのもとに、上司である茂礼手課長から「至急確認してほしい」というメールが届いた。普段はチャットや口頭で依頼されるのに、今日は添付ファイル付きのメールで連絡が来ている。なんだかいつもと様子が違うのだが、よく知る上司からの連絡なので、すぐに対応しようと思う。

Q 下の選択肢から適切なものを選ぼう！

1. すぐに添付ファイルを開く
2. 送信元のアドレスを確認し、
   問題なければ添付ファイルを開く
3. 電話やチャットで上司に確認する

03
A

3 電話やチャットで上司に確認する

こうしたメールは、**ビジネスメール詐欺（BEC）や標的型攻撃メール**の可能性があります。
上司や取引先のほか、役職者や管理部門からの依頼を装い、添付ファイルの開封を促すのは「なりすまし」の常套手口で、ウイルス感染や情報窃取の危険があります。

解　説

ビジネスシーンでは、送金や振込を依頼してくるビジネスメール詐欺（BEC）や、添付ファイルやリンクを開かせてウイルス感染や社内システム侵入をはかり、情報窃取や長期的な攻撃に発展させる標的型攻撃が見られます。普段やりとりしている相手に限らず、社長や本部長などの役職者、人事や経理といった管理部門を装い、緊急性を強調して即時対応を迫る例もあります。

- ✓ **送信元アドレスの偽装や不正利用の可能性もあるため、電話やチャットで本人に確認を取る**
- ✓ **万が一、添付やリンクを開いてしまった場合には速やかに上司や情報システム担当者にすぐに相談する**

相手や連絡手段、内容が「いつもと違う」というのがポイントにゃ！
アドレスは偽装や乗っ取りの可能性があり、さらに最近は、生成AIで誰でも自然な文章を作れるようになったので、送信元や明らかに不自然な言葉遣いだけで見抜くことも難しくなっているにゃ…。

04 よく利用する宅配業者から再配達手続きのメッセージが届いた

通販サービスで買い物をすることが多いのに、仕事で家を不在にしていることも多い茂礼手課長。いつも荷物を届けてくれる宅配業者から「こちらのリンクから再配達の手続きを行ってください」というメッセージが届いた。直近は何か買った覚えはないのだが、とりあえずメッセージに従い、再配達手続きをしようと思う。

Q 下の選択肢から適切なものを選ぼう！

1. メッセージに従い、リンク先の画面で配達希望の自宅住所などを入力する

2. 公式サイトや公式アプリを直接開き、自分宛ての荷物がないか確認する

04

A

2

公式サイトや公式アプリを直接開き、自分宛ての荷物がないか確認する

宅配業者など、身近でよく利用するサービスを装ったメッセージは「**フィッシング詐欺**」の典型です。リンク先で住所やメールアドレスなどの個人情報を入力してしまうと、不正利用や金銭的被害につながる危険があります。

解　説

他にも、「アカウントの再認証を行ってください」「不正アクセスがあったので、状況を確認してください」「パスワードを更新してください」など、身近にありそうなメッセージが多く見られます。ワクチン接種や税金・還付金・給付金など、時事ニュースと関連させた手口も多く確認されているため、受け取ったメッセージには常に警戒心を持ちましょう。

- ✓ **受け取ったメッセージには常に警戒心を持つ**
- ✓ **公式サイトや公式アプリに直接アクセスし、サービスからの通知を自分で確認**

入力された情報は、攻撃者同士で売買されることもあり、クレジットカードの不正利用や銀行口座からの不正送金、さらに他サービスへの不正ログインにも使われる可能性があるにゃ。小さな油断が大きな被害につながるにゃ。

05 QRコードが載った災害復興支援募金のポスターを見かけた

大きな地震のニュースに心を痛めているます子さん。そんなとき、街で「災害復興への支援募金」の呼びかけポスターを見かけた。ポスターには、被害に遭った地域への支援を求めるメッセージと、募金サイトへのQRコードが記載されている。ぜひ募金をしたいので、すぐにスマホでQRコードを読み取ろうと思うが…。

Q 下の選択肢から適切なものを選ぼう！

1. QRコードを読み取り、
表示された募金サイトですぐに送金する

2. QRコードからではなく、
支援団体の公式サイトから募金方法を確認する

05
A

2 QRコードからではなく、支援団体の公式サイトから募金方法を確認する

スマホのカメラで手軽に読み取れるQRコードを悪用した詐欺を「**クイッシング（QRコードフィッシング）**」といいます。読み込んだ先でQRコード決済や情報入力を求められ、情報や金銭をだまし取られる危険があります。

解　説

募金チラシや公共料金の請求書、再配達伝票などを装い、偽のコードを印字して配布する手口のほか、正規のQRコード決済の案内板に偽のコードを貼付する手口に注意が必要です。偽サイトや攻撃者に送金される決済画面へ誘導されたり、メッセージのやりとりでQRコード決済の画面のスクリーンショットを送るよう求められ、情報や金銭をだまし取られる被害が発生しています。

- ✓ **安易にQRコードからアクセスしない**
- ✓ **公式サイトや公式アプリから確認しに行くひと手間を挟む**

スマホの読み取り機能によっては、QRコード化されているURLの文字列を確認できない仕様のものがあるにゃ。文字列が見慣れなかったり、公式と異なっていたりすることに気づけば被害を防げるので、URLを読み取りしてくれるアプリを使おうにゃ！

06 覚えるのが大変なので、複数のサービスで同じパスワードを使い回している

最近は、どんなサービスも桁数や文字の種類が多い複雑なパスワードを設定するよう求めてくる。さすがに覚え切れなくなってきた茂礼手課長は、しっかり考え抜いた十分に長い文字列のパスワードだから、破られはしないだろうと思い、複数のサービスでこのパスワードを使い回している。

Q 下の選択肢から適切なものを選ぼう！

1. 問題はない
2. 問題がある

06

A

2 問題がある

十分に長いパスワードであっても、複数のサービスで同じパスワードを使い回すことは大きなリスクです。どこか一つのサービスでパスワードが漏洩すると、攻撃者に同じパスワードを使って他のサービスへも不正ログインされ、被害の連鎖を招く危険があります。

解　説

攻撃者は、漏洩したユーザー名とパスワードの組み合わせを用いて別のサービスに侵入する「パスワードリスト攻撃」を仕掛けてきます。こうした攻撃による被害を連鎖的に拡大させる危険な行為です。

- ✓ **パスワード管理アプリで、サービスごとに異なる十分に長いパスワードを作成し、管理する**
- ✓ **生体認証や多要素認証も設定しておく**

特にメールのアカウントは、多くのサービスのログインIDになっていたり、二段階認証やパスワード再設定の通知先になっているので超重要！

07 多要素認証の設定を求める通知が届いた

利用しているオンラインバンキングサービスから「多要素認証を設定してください」というメールが届いているます子さん。「セキュリティ向上と不正ログイン防止のため」という案内だが、毎日いろいろ忙しく、改めてサービスの設定を見るのが手間なので、しばらく放置している。

Q 下の選択肢から適切なものを選ぼう！

1. 問題はない
2. 問題がある

07

A

2 問題がある

「多要素認証」は、パスワードの他に別の認証要素を組み合わせることで、不正ログインのリスクを大幅に減らせる非常に重要な対策です。未設定のままだと、万が一パスワードが漏洩したときに、攻撃者に簡単にアクセスされてしまいます。

解　説

組み合わせる要素には、パスワードやPINコードのような「知っているもの」、SMSで確認コードが届くスマホやトークンのような「持っているもの」、顔や指紋といった「本人そのもの」などがあります。それぞれは突破される可能性があっても、異なる種類を重ね合わせることで、攻撃者はすべてを同時に突破することが極めて困難になります。

✓ **サービス利用開始時、セキュリティ機能の追加案内があればすぐに設定をする**

…と言いつつ、「多要素認証を設定してください」というメッセージの中には、
正規の銀行やサービスを装ったフィッシング詐欺もあるにゃ…。
公式サイトや公式アプリから設定画面を確認しよう！

08 部署のメンバー全員で業務システムの管理者アカウントを共有している

茂礼手課長・ます子さんの部署で使用している業務システムは、本来は担当者ごとに閲覧権限や操作権限を設定できる仕様になっている。しかし、課長は「担当者不在のときに業務効率が落ちてしまうから…」と、管理者権限のID・パスワードを部署のメンバーに共有している。

Q 下の選択肢から適切なものを選ぼう！

1. 問題はない
2. 問題がある

08

A

2 問題がある

ID・パスワードを共有すると、システムへのアクセスや「誰が・いつ・何をしたか」の追跡ができず、不正利用や情報漏洩が発生したときに原因特定が困難になります。特に管理者権限は影響範囲が大きいため、メンバーごとにIDと権限を個別に設定し、適切に管理する必要があります。

解　説

複数人で共有すると誤操作や不正の追跡が困難になるだけでなく、退職者が利用できる状態のままとなり、内部不正のリスクも高まります。そのため、各メンバーに個別IDを発行し、必要最小限の権限を付与することが原則です。

- ✓ **定期的にアカウントの見直しをする**
- ✓ **退職や異動時には速やかにアカウントを無効化・削除する**

おすすめはしないけど、やむを得ずパスワードを共有している場合、定期的にパスワードを変更し、退職者や異動した人を除いて、その時点で本当にアクセスが必要な人だけに共有することが、最低限の対策にゃ！

09 SNSで写真・動画の投稿やタグ付けを頻繁に行っている

友達とつながれるし、「いいね！」をもらえると嬉しいし、流行りの情報もすぐにキャッチアップできるので、毎日欠かさずSNSをチェックしている茂礼手課長。子どもの成長記録や日常の写真や動画をたくさん撮って、皆に思い出やつながりをシェアしようと、場所や友人をタグ付けして投稿している。

Q 下の選択肢から適切なものを選ぼう！

1. 公開範囲を全体にして、
できるだけ多くの人に見てもらう

2. 位置情報や友人のタグ付けを含め、
内容ごとに公開範囲を見直す

09

A

2

位置情報や友人のタグ付けを含め、内容ごとに公開範囲を見直す

SNSは便利なツールですが、設定を確認せずに使い続けると、何気ない投稿から個人情報が推測され、プライバシー侵害や犯罪被害につながる危険があります。

解　説

SNSに投稿した写真や動画は、背景や写り込みから自宅や勤務先、学校などが特定されたり、位置情報のタグ付けから現在地が知られたりするおそれがあります。また、写真に一緒に写ったり、タグ付けされたりしている友人や家族についても、本人の承諾なしにプライバシーをさらしてしまうことになりかねません。

- ✓ **公開範囲やタグ付けなどの設定を事前に確認する**
- ✓ **あらかじめサービスの設定から全体的に適切な公開設定にしておく**
- ✓ **投稿時には内容に応じて非公開や限定公開、タグの有無を使い分ける**

ネットに一度公開した情報は「デジタルタトゥー」として残り続け、将来思いがけないトラブルにつながることがあるにゃ。設定をよく確認せずに投稿すると、思わぬ人にも見られてしまうから注意するにゃ。

10 ソフトウェアの更新通知が来ているのにスルーしている

会議資料の作成で忙しい茂礼手課長のPCに、また「ソフトウェアを最新バージョンにアップデートしてください」という通知が。別に古いソフトでも業務に支障は出ていないし、毎日会議に追われている中、更新作業は時間が取られて手間なので後回しにしているのだが…。

Q 下の選択肢から適切なものを選ぼう！

1. 通知を無視して、そのまま使い続ける
2. 通知設定をOFFにする
3. すぐに最新の状態に更新する

10
A

3 すぐに最新の状態に更新する

ソフトウェアのアップデートは、脆弱性を修正し、セキュリティを強化する重要な作業です。
更新を怠っていると攻撃者に脆弱性を悪用されるリスクが高まります。

解　説

OSや各種アプリなど、ソフトウェアには、開発段階で意図せず生じたセキュリティ上の欠陥、いわゆる「脆弱性」が潜んでいる可能性があります。古いまま使い続けると、その弱点が放置され、攻撃者に悪用される危険が高まります。不正にアクセスされたり、ウイルスを仕込まれ、情報を盗まれたりするだけでなく、さらなる攻撃の踏み台にされるリスクもあります。

✓ **通知が来たら後回しにせず、常に最新の状態に更新し続ける**

通知が来ると「業務中に手間だな…」と感じるかもしれないけど、自動更新やバックグラウンド更新もできるので、設定を見直しておこうにゃ！ スマホも、Wi-Fi接続時や就寝している夜間・充電中にアップデートできる設定があるにゃ。

11 サポートが終了したバージョンのOSを使い続けている

長年使い慣れたOSを、何も気にせずそのまま使い続けている茂礼手課長。部下のます子さんから「課長！ OSのサポート切れてます」と指摘されたが、今日もやるべき仕事が満載で、「アップデートって時間がかかるし面倒だな…」「見慣れた画面が変わると嫌だな…」と思っている。

Q 下の選択肢から適切なものを選ぼう！

1. 今まで問題なかったので、
サポートが終了したOSをそのまま使い続ける

2. 念のため、ウイルス対策ソフトだけ更新しておく

3. 速やかに新しいOSにアップデートする

11
A

3 速やかに新しいOSにアップデートする

OSのサポート終了後は、脆弱性を修正するためのアップデートが提供されなくなり、脆弱性が残ったままになります。これにより、脆弱性を悪用した攻撃を受けるリスクが急増します。

解　説

OSだけでなく、ソフトウェアやアプリも同様です。特にサポート終了によりアップデートが止まると、それ以降は脆弱性が修正されなくなってしまいます。サポートが終了したソフトウェアやアプリの使用は、脆弱性を悪用した攻撃のリスクを高めるため、速やかにサポート対象の最新バージョンへの移行が必要です。

- ✓ **ウイルス対策ソフトに頼らず、必ず速やかに最新バージョンのOSにアップデートする**
- ✓ **スマホやPCの機種が古く、新しいバージョンにアップデートできない場合は、買い替えも検討する**

サポート切れのOS やアプリは、言わば“むきだし”の状態で、攻撃者の恰好の標的！必ずアップデートしよう。ウイルス対策ソフトはウイルスの検知に役立つもので、脆弱性そのものを直せるわけではないにゃ…。

12 全体公開でSNS投稿している

ます子さんも、仕事にも役立つ情報や人脈を得られるので、SNSを好んで使っている。ある日、友人から「オフィスで仕事している写真、誰でも見られる状態になっているよ、大丈夫？」と指摘されてしまった。「誰かとつながれるといいな」「自分の投稿が誰かの役に立つといいな」と思い、全公開で投稿していたのだが…。

Q 下の選択肢から適切なものを選ぼう！

1. これまで通り、プライベートも仕事のことも全公開で投稿する
2. 投稿前に、会社の機密や他者のプライバシーが含まれていないか確認する

12

A

2

投稿前に、会社の機密や他者のプライバシーが含まれていないか確認する

SNSや情報発信をやめる必要はありませんが、すべてを公開してしまうのは大きなリスクを招きます。会社の内部情報や他者のプライバシーにつながることは不用意に公開すべきではありません。

解　説

社内の風景や資料の写り込みは機密情報の漏洩に直結します。また、他社への訪問や出張、残業状況などの情報も、業務内容を推測される可能性があります。さらに、関係者や同僚の写真を本人の同意なしに公開することはプライバシー侵害にもなりかねません。こうした情報は詐欺やストーカーにつながったり、競合企業や企業へのサイバー攻撃を企む攻撃者の情報収集に悪用される恐れがあります。

- ✓ **会社の内部情報や他者のプライバシーにつながることは不用意に公開しない**
- ✓ **会社ルールや社会的モラルに従い、投稿前に内容を確認する**

「デジタルタトゥー」になって半永久的に残ってしまうから、自宅や家族・友人のこと、会社や仕事のことなど、他者に知られてはいけない、知られたくない内容は発信前に「公開して本当に大丈夫か」必ず考えてにゃ！

13 カフェでリモートワーク中、PC画面を隠さず作業している

外出や出張が多く、駅の待合スペースやカフェでよくリモートワークをしている茂礼手課長。最近は観光客も多く、どこも混雑しているが、訪問や移動の合間に少しでも仕事を進めておきたいので、PCを開いて作業に没頭している。

Q 下の選択肢から適切なものを選ぼう！

1. リモートワークの許可は出ているので、そのまま画面を隠さずに作業を続ける
2. 念のため、画面を見ないでほしいと周囲の人に声を掛ける
3. 画面に覗き見防止フィルムを付け、壁を背にした席に座る

13

A

3

画面に覗き見防止フィルムを付け、壁を背にした席に座る

公共の場では、スマホやPC画面に映った情報を周囲の人に“覗き見（ショルダーハック）”されるリスクがあります。

解　説

駅や空港、車内や機内、カフェなど公共の場では、意外と周囲からスマホやPCの画面が見えてしまい、覗き見による情報漏洩のリスクに繋がります。

- ✓ **横からの視線を遮ることができるプライバシーフィルターやプライバシーフィルムを使う**
- ✓ **スマホにカバーを付けたり、画面を伏せて置く、壁や柱を背にして座る、画面を暗めに設定する**
- ✓ **外部で作業してよい内容や、作業自体を制限している場合もあるため、必ず職場のルールを確認する**

パスワードやクレジットカード情報などの重要情報は、職場や自宅など、不特定多数の人がいない場所で入力する、入力時に画面や手元を見られていないか周囲を警戒する、といった心がけも大切にゃ！

14 私物のUSBメモリを業務で使用している

外出先で急いで仕事相手にデータを渡す必要があったます子さんは、つい私物のUSBメモリを使ってしまった。特に問題は起きていないし、「急ぎだったし、この案件だけだから…」と、そのままデータのやりとりに使用し続けている。

Q 下の選択肢から適切なものを選ぼう！

1. 私物のUSBメモリを使い続ける
2. 私物のUSBメモリはさすがによくないので、私用のクラウドストレージにする
3. 業務用のUSBメモリを使用する

14
A

3 業務用のUSBメモリを使用する

会社の管理下にない私物のUSBメモリの業務利用は、ウイルス感染や紛失による情報漏洩リスクが高く、不適切です。また、私用のクラウドストレージも管理や安全性の観点から不適切です。

解　説

私物のUSBメモリや私用のクラウドサービスの利用は、会社がリスクを管理・把握できない「シャドーIT」となります。業務データは個人の利便性を優先するものではなく、組織全体で守るべき大切な資産です。「急ぎだったから」「今回だけだから」という言い訳は繰り返しを招き、組織全体のセキュリティを揺るがしてしまいます。

✓ **会社のルールや申請方法に従い、指定の方法でデータを保存・共有**

会社が把握していない私物のUSBメモリや私用のクラウドサービスなどは「シャドーIT」と呼ばれるにゃ。見えないリスクがいっぱい潜んでいるから、便利だからって使っちゃダメ！

15 SNSで拡散希望が流れてきたのでそのままリポストした

災害により大きな被害が出ているようで、SNSで「緊急！」「拡散希望！」の情報が流れてきた。「困っている人を助けるぞ！」と、リポストした茂礼手課長。しかし後日ニュースを見ると、誤情報で現場は大混乱に陥り、救助活動に支障が出ていた模様。あの時リポストしてしまったけど、本当はどうするべきだった…？

Q 下の選択肢から適切なものを選ぼう！

1. 行政の発表やニュースなどで
情報の真偽を確認してからリポストする

2. そのまま流れてきた情報をリポストする

15
A

1

行政の発表やニュースなどで
情報の真偽を確認してからリポストする

災害時に大切なのは、不確かな情報を広めず、正しく確認された情報を届けることです。
真偽を確認せずに発信すると、混乱や誤解を招き、本当に必要な支援や救助活動を妨げる恐れがあります。

解　説

情報発信には社会的な影響力が伴い、よかれと思っての拡散であっても、誤った情報発信は結果的に混乱を助長させてしまいます。
実際、一度拡散された古い情報が、まるでいま起きていることのように流れてくるデマや、いたずら目的で架空の情報を拡散する事例が数多く起きています。

- ✓ **流れてきた情報を鵜呑みにしない**
- ✓ **行政やメディアなどの公式発表の内容を確認する**
- ✓ **デマに加担しない、「いま必要な正しい情報か」を見極めて行動する**

巧妙な写真の合成や、AI を悪用して本物そっくりの偽の映像や音声を生成するディープフェイクの問題も深刻にゃ。見た目や音声だけで信じ込まず、情報の裏付け確認が欠かせないにゃ。

16 データを買いたいという怪しいメールが届いた

最近、何かと仕事が上手くいかなくて、疲れていた茂礼手課長。そこに、「短期でまとまった報酬を保証。顧客リスト譲渡のご相談」というメールが届いた。「それくらいなら…」と心が揺らぐが…。

Q 下の選択肢から適切なものを選ぼう！

1. メールの誘いに応じてデータを提供する
2. メールは無視し、上司や担当者へ報告する

16

A

2 メールは無視し、上司や担当者へ報告する

会社の情報や顧客リストを外部へ渡す行為は、不正競争防止法や個人情報保護法に違反し、刑事罰や高額な損害賠償につながる重大な不正行為です。

解　説

会社の機密情報や顧客リストを無断で外部に提供する行為は、組織に対する背信行為であり、重大な法的責任を伴います。短期の報酬につられると、刑事罰や高額な損害賠償につながるおそれがあります。こうした勧誘は、詐欺やスパイ活動の入り口であることも多く、ちょっとしたやり取りでも情報漏洩や不正行為に発展する可能性があります。会社の情報は会社の大切な資産であって、個人のものではありません。

- ✓ **メッセージを受信したら無視して削除し、速やかに上司や情報システム担当者へ報告**
- ✓ **甘い誘いには乗らないという強い意志を持つ**

退職や転職のタイミングは、気持ちが揺れやすく狙われやすいにゃ。次の職場への準備や不安につけ込まれて「情報を持ち出してほしい」と誘われてしまったケースもあるにゃ。

17 電車の中にスマホを置き忘れた

電車にスマホを置き忘れてしまった茂礼手課長。スマホには連絡先や写真、メールや会社のチャット、SNS、キャッシュレス決済など、仕事やプライベートの情報が詰まっている。「スマホがないと何もできない！」と慌ててしまったが、まず何をすべき…？

Q 下の選択肢から適切なものを選ぼう！

1. 自分で探す
2. 駅の忘れ物センターや警察に相談して、遺失届を出す
3. 紛失モードを有効にし、キャリアや決済も利用停止

17
A

3

紛失モードを有効にし、キャリアや決済も利用停止

スマホを紛失したとき、最も大切なのは情報漏洩や不正利用を防ぐための“初動”です。

解　説

端末や端末に入っている情報を守り、リスクの最小化を図るために、紛失モードやリモートロックで第三者の操作を防ぎながら、端末の位置を確認しましょう。

- ✓ **まず最優先で端末の「紛失モード」やリモートロックを有効化にする**
- ✓ **キャリアに連絡し、決済サービスを使っている場合には、それらの利用停止手続きやパスワード変更を行う**
- ✓ **「戻ってこない可能性が高い」場合には、リモートワイプで端末内のデータを消去する**
- ✓ **並行して駅や警察に遺失届を出し、業務用端末なら、速やかに上司や情報システム担当者に報告する**

日頃から、画面ロック（パスワードやPINコード、生体認証）の設定やデータのバックアップを徹底しておくことも大切だにゃ。

18 メールの誤送信で、取引先に関係のない機密資料を送ってしまった

社内のメンバー宛てのメールを、うっかり取引先に誤送信してしまった茂礼手課長。しかも添付ファイルには、まだリリースしていない新商品の資料や顧客情報などの機密情報も含まれていた。どうしたらよいだろうか…。

Q 下の選択肢から適切なものを選ぼう！

1. いつもよくしてくれる相手だし、「まぁ大丈夫だろう」と放置する
2. 個人的に連絡し、そっと削除してもらえるようお願いする
3. すぐに上司に報告し、削除依頼など、しかるべき対応をする

18

A

3

すぐに上司に報告し、削除依頼など、しかるべき対応をする

機密情報を誤って外部に流出させてしまった場合は、速やかに上司へ報告し、
組織的な対応をする必要があります。

解　説

社外秘の新商品企画や技術情報・価格情報など、取引先や顧客の情報といった外部に知られてはならない情報が流出すると、最悪の場合、取引停止や損害賠償などにつながるおそれがあります。人事情報や業績データのように主に社内向けの情報が誤って流出した場合でも、信用失墜は避けられません。

- ✓ **自己判断・自己解決で終わらせない**
- ✓ **誤送信に気づいたら、まずはすぐに上司へ報告し、必要に応じて情報システム担当者や個人情報管理の担当者などとも連携して、組織としての対応をとる（ストレージでの送信ならリンクの無効化、直接の添付なら削除依頼など）**

メール送信前に送付先や添付ファイルをチェックしたり、送信ボタン押下後も実際の送信を一定時間保留する機能なんかもあるにゃ。メール誤送信の防止策として、こうした補助ツールも利用しよう！

19 業務中に不審なメールが届いたが、すぐ削除した

業務中に、身に覚えのないメールがます子さんのもとに届いた。不審メールだと気づき、開封せずにすぐ削除したので、ウイルス感染などのトラブルも起きていない様子。このまま一件落着としてよい…？

Q 下の選択肢から適切なものを選ぼう！

1. 社内ルールに従い、
上司や情報システム担当者に報告する
2. 一件落着で問題なし
3. メールを再度開いて内容を確認する

19

A

1

社内ルールに従い、
上司や情報システム担当者に報告する

最近の攻撃メールは本物そっくりで判別が難しく、個人の対応だけでは十分とは言えません。
ほかの社員にも同様のメールが届いている可能性があります。

解　説

うっかりリンクや添付ファイルを開くと、ウイルス感染、情報漏洩、アカウント乗っ取りなどの被害に遭うだけでなく、
あなたのスマホやPCが「攻撃の踏み台」にされ、会社や組織全体に被害が拡大してしまうケースがあります。

- ✓ **社内で定められた報告フローを確認し、速やかに報告する**
- ✓ **報告によって全社員への注意喚起やフィルタリング強化など組織的対策につながります**

最近は、攻撃者がメールに追跡機能を仕込んでいることもあるにゃ。「誰が・いつ・開封したのか」を把握され、開いただけで次の攻撃のターゲットにされる可能性があるにゃ。

20 突然、登録完了画面が表示され、支払いを求められた

スマホでWebサイトを閲覧していた茂礼手課長。すると突然、「会員登録が完了したので、動画視聴が可能になりました」という画面が表示され、支払い手続きを求められた。

Q 下の選択肢から適切なものを選ぼう！

1. 記載された連絡先に問い合わせて確認する
2. とりあえず請求金額を支払ってしまう
3. 登録や利用の事実がなければ無視し、画面を閉じる

20
A

3 登録や利用の事実がなければ無視し、画面を閉じる

実際には契約も登録もしていないのに「完了した」と表示し、不安をあおって金銭をだまし取るのは
「**ワンクリック詐欺**」の典型的な手口です。
電話やメールで連絡して個人情報を渡してしまうと、さらなる請求や別の詐欺に発展するおそれがあります。

解　説

実際には契約は成立しておらず、支払う義務も一切ありません。

✓ 無視して画面を閉じることが正しい対応

クレジットカードや電子決済の利用明細などを確認して「実際に被害が発生している」場合は、消費者ホットライン（188）や警察庁「サイバー事案に関する相談窓口」に相談してにゃ！

NO MORE 情報漏洩2050

「共創型」セキュリティ啓発プロジェクト

ABOUT

**MOTEXは、すべての人が安心してデジタル技術を活用できる、
セキュアな社会の実現を目指しすべく、**

**共創型のセキュリティ啓発プロジェクトとして、
『NO MORE 情報漏洩 2050』を推進しています。**

『NO MORE 情報漏洩 2025』プロジェクトでは、公式SNSやブログで
さまざまな情報を発信しています。ぜひご覧ください。

X　Facebook　note

改訂履歴

版	発効日	改版内容
第1版	2017年2月23日	初版発行
第1.1版	2017年4月5日	P8 ：「情報セキュリティ10大脅威」を2017版に更新 P17：画像差し替え P32：表記修正
第2版	2018年2月19日	P7 ：「セキュリティ事故（情報漏えい事故）がもたらす影響」を更新 P8 ：「情報セキュリティ10大脅威」を2018版に更新 P10：「標的型メール攻撃」を更新 P11：「過去最大級のインシデント、ランサムウェア被害」を追記 P13：「過失による情報漏えい」を更新
第3版	2019年2月12日	P7 ：「セキュリティ事故（情報漏えい事故）がもたらす影響」を更新 P8 ：「情報セキュリティ10大脅威」を2019版に更新 P10：「標的型メール攻撃」を更新 P13：「過失による情報漏えい」を更新
第4版	2021年8月31日	P7 ：「セキュリティ事故（情報漏えい事故）がもたらす影響」を更新 P8 ：「情報セキュリティ10大脅威」を2021版に更新 P13：「無くならないランサムウェア被害・新種ウイルス被害」を追加
第5版	2026年2月2日	全内容刷新