NO MORE 情報漏洩 2050

「共創型」セキュリティ啓発プロジェクト

『NO MORE 情報漏洩 2050』プロジェクトは、エムオーテックス株式会社が推進する共創型のセキュリティ啓発プロジェクトです。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ています。

非売品

MOTEX

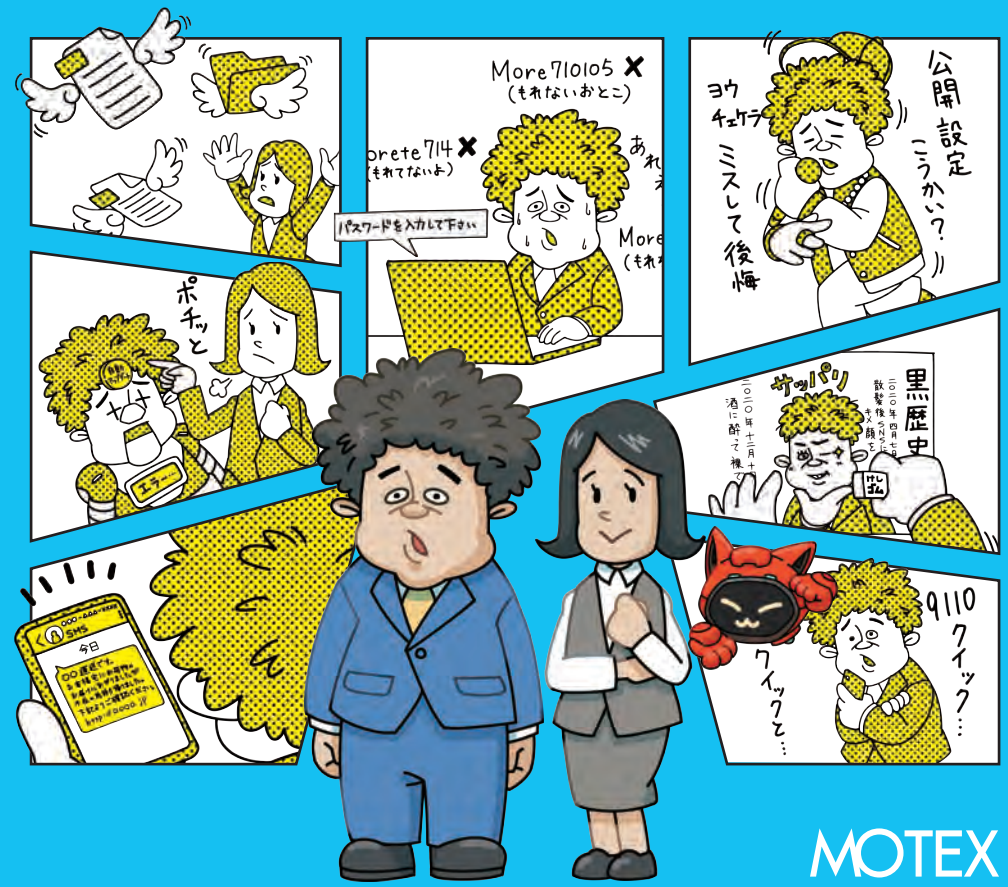
発行：エムオーテックス株式会社

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

サイバーセキュリティハンドブック

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



MOTEX

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

登場人物紹介

バンニャ
BANNYA

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。

もれて　たろう
茂礼手 太郎

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。

ふせぎ　ますこ
布施木 ます子

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…

\ 教育担当者向け /

社員教育で使える！ セキュリティ教育コンテンツ

企業や学校で、セキュリティ研修・教育を担当されている方々向けに、サイバーセキュリティハンドブックをもとにした教育コンテンツをご用意しました。
教育資料とテストを活用し、定期的なセキュリティ教育・マナー研修を実施することで、一人ひとりのセキュリティリテラシーを向上させ、さらにポスターを活用することで、セキュリティ意識を習慣化できます。
ぜひセキュリティ教育にご活用ください。

教育資料（講師用）

サイバーセキュリティハンドブックの内容をもとにした講師の方向けの資料です。
本書には掲載されていない、時事ネタや情報が含まれています。PPT形式で編集ができるため、自社向けにカスタマイズして資料が簡単に作成できます。

テスト

サイバーセキュリティハンドブックの内容をもとにしたテストです。
研修後の復習や理解度確認のためにご活用ください。
Microsoft　Formsへのインポート、もしくはGoogleフォームをコピーすることで簡単にテストを作成できます。

ポスター

セキュリティ 7つの習慣を載せたポスターです。会社や学校で壁に貼って、日常的なセキュリティ意識向上のためにお役立てください。

各種コンテンツは全て無償でダウンロードいただけます！

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？

本書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、
サイバーセキュリティハンドブックです。

初版は2016年に発刊し、これまでに3万部以上ダウンロードいただいておりますが、
社会情勢の変化や技術革新が進み、
セキュリティに関する知識もアップデートが求められています。
そこでこのたび、ゆる～いイラストや楽しいクイズで優しく学べる構成はそのままに、
内容を全面的に見直し、第二版としてリニューアルしました。

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。

また、本書をもとにしたセキュリティ教育コンテンツも無料でダウンロードいただけます。
会社や学校でのセキュリティ教育やマナー研修などにぜひご活用ください。

2026年2月

エムオーテックス株式会社

目次

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」は、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です。

「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。
一方、「なりすまし詐欺」は、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です。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」は、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、非常に悪質な手口です。

攻撃者は事前にターゲットの情報を念入りに調べ、取引先や社内外の関係者を装い、あなたが疑わない相手になりすまします。送られてくるメールやメッセージは、請求書や資料共有、人事通知など、ごく自然で、まったく怪しさを感じさせない内容で巧妙にカスタマイズされています。
うっかり不審なリンクや添付ファイルを開きウイルスに感染すると、情報漏洩やアカウント乗っ取りを招きます。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。
こうした手口にだまされないためには、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、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、必ずチェックしましょう。

POINT 3

「今すぐ！」と言われてもひと呼吸おこう

最近、「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サイト上で表示する「サポート詐欺」が発生しています。

これは「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です。画面全体を覆うポップアップや大音量のアラート音で不安をあおられ、案内に従ってしまうと、偽のサポート窓口に誘導されます。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の被害につながります。
まずは慌てず、冷静に状況を疑うことが重要です。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。自分で対応が難しい場合は、画面に表示されている電話番号には絶対に連絡せず、情報システム担当者や警察に相談してください。

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。
ここでは、いますぐ使えるチェックポイントを紹介します。

☑ リンクを安易にクリックしない

メッセージ内のリンクは偽サイトへ誘導されるリスクがあるため、公式アプリや公式サイトから内容を確認しましょう。
よく利用するサービスは、ブックマークやお気に入り、ショートカットなどに登録し、“自分で保存した正規URL”からアクセスする習慣をつけると安全です。

☑ 広告や見慣れないサイトへのリンクに注意

SNSや検索結果に表示される広告から、有名ブランドをかたった偽サイトへ誘導する手口が増えています。
「1万円キャッシュバック」「90%OFF」など、過剰に“お得すぎる”表示には特に注意が必要です。

☑ 送信元を確認する

メールアドレスや差出人名は簡単に偽装されるため、見た目だけで判断しないことが大切です。

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

正規のサービスが、ID・パスワード・個人情報・支払情報をメールやSMSで入力させることは、極めてまれです。メッセージから開いた画面で入力を求められても、絶対に入力しないでください。
行政機関や金融機関をかたったフィッシングが急増しているため、特に注意が必要です。

☑ 迷ったら公式サイトから確認する

少しでも不安を感じた場合は、メッセージ内のリンクや電話番号は使わず、公式サイトで公表されている正規の問い合わせ先から連絡して真偽を確認しましょう。
電話の場合は「発信元番号の偽装（なりすまし）」もあるため、受け身にならず自分で正規窓口に電話をかけることが大切です。

標的型攻撃メールに注意！
メールの安全性を確認する方法を身につけよう

業務でも日常でも、身近な連絡手段である「メール」。
最近は詐欺メールだけでなく、業務連絡を装った「標的型攻撃メール」も増えています。
年々巧妙化しており、“一見ふつう”で“関係者からの連絡に見える”ものでも、実は攻撃メールだったというケースも珍しくありません。
「うっかり開封」を防ぐために、受信メールの安全性を確認する3つのポイントを身につけましょう。

超重要 メールの安全性を確認する方法

差出人	○○本部長＜xxx@hogehoge.jp＞
件名	重要：下期方針について
本文	各位 お疲れ様です。 ○○です。 下期方針に関する補足の資料を送付します。 各自、以下のリンクより必ずご確認をお願いします。 下期方針の補足 ○○

①差出人メールアドレス

差出人の表示名とアドレスが正しい組み合わせか、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、受信者に開封させるため、「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」といった業務上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。

こうした不審メールを受信したら開封せずに削除し、もし開封してしまった場合は、速やかに上司や情報システム担当へ相談しましょう。
また、攻撃メールは特定の1人だけに届くとは限らず、誰か1人が受信している場合、他の社員にも同じ攻撃メールが届いている可能性があります。不審メールの受信や気になる挙動があった際には、些細なことでも周囲に報告・共有することが、組織全体を守ることにつながります。

怪しいメールは、開けても開けてなくても“すぐ報告”！
1人に届いていたら、他の仲間にも届いているかもしれないにゃ！

習慣 2

投稿が誰から見られているか意識しよう

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で何かを発信するときは、ちょっと立ち止まって考えてみてください。その投稿の中に、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？

なにげない写真や動画でも、実は写っている背景からあなたの行動範囲や居場所がバレてしまうことがあります。特に、位置情報がオンになっていると、あなたの居場所が簡単に特定されてしまいます。
また、自分がよくても友人・知人・家族が写っている写真や動画の投稿、タグ付けも要注意です。他人のプライバシーに関わる情報を、相手が知らないところで勝手に公開してしまうことになります。
発信する前には必ず相手の承諾を得るようにし、他人のプライバシーにも配慮しましょう。

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。

例えば、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ことがあります。たとえ断片的な情報でも、あなたがどこの会社でどんな立場なのか、どんな仕事をしているのかを知られてしまうと、それらの情報がつなぎ合わされ、会社の動向が筒抜けになってしまうこともあります。

また、内輪の話や不満をSNSでつぶやくことは、職場や組織のイメージを大きく損なうだけでなく、無意識のうちに社外秘の情報をさらしてしまうことになりかねません。

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」と常に意識しましょう。

POINT 3

「デジタルタトゥー」になり得ることを意識しよう

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。これが「デジタルタトゥー」です。

例えば、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てしまうのです。

また、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よくあります。

こうしたデジタルタトゥーや炎上のリスクを意識し、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？」と投稿を見直してみましょう。

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。

「私は非公開アカウント（鍵アカウント）だから大丈夫」と思っている人もいるかもしれませんが、油断は禁物です。非公開アカウントであっても、他のサービスと連携していると、思わぬところで投稿が表示されることがあります。また、非公開アカウントの内容を誰もが閲覧できる公開の場に転載してしまい、それが炎上につながるケースもあります。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、必要な設定に変更しましょう。

コラム

よく考えよう、情報の信憑性

ネットの情報、鵜呑みにして大丈夫？賢く見極める目を養おう

インターネット上には、誤った情報やデマが溢れています。日々流れてくるSNSやニュースを見ていると、どれが本当の情報なのか分からなくなることが多くあります。

例えば、災害時にはウソの被害状況を伝えるデマ情報が広まり、救助活動の妨害や現場の混乱を招く事態が実際に発生しました。最近はAI技術の進化により、「ディープフェイク」と呼ばれる本物そっくりの画像や動画を簡単に作れるため、政治家や有名人の発言、事件・事故の状況など、一見信頼できそうに見えても実はデマだった、なんてことも珍しくありません。

こうしたデマ情報は、特にSNSを通して広がりやすく、根拠のない話でも拡散されるうちに本当のことのように伝わってしまいます。その結果、企業の株価に影響を及ぼしたり、不買運動につながったりした事例もあります。

ネットの情報を鵜呑みにするのはとても危険です。大切なのは、「これは信頼できる情報か」と見極める目を養うことです。そして、情報を発信する際は、発信者としての責任を持ち、次の原則を守りましょう。

根拠のない情報は拡散しない

根拠のない情報や疑わしい情報を広めることは、社会に混乱をもたらし、多くの人に迷惑をかける可能性があります。安易に拡散しないようにしましょう。

情報の出どころを確認する

行政機関や企業からの公式発表、信頼できるメディアからの報道、専門家の発信などを参考にしましょう。

複数の情報源を比較する

確かな根拠を得るため、いくつかの情報源を比べたり、発信元の実績や評判をチェックしたりしましょう。

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。

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、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を利用するようにしましょう。もしあなたが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。

このようなリスクを防ぐため、ぜひ「パスワード管理アプリ（パスワードマネージャー）」を活用しましょう。このツールは、強力なパスワードを自動生成・管理してくれる上、各サービスのログイン時に必要なIDとパスワードを提供してくれるので、あなたは自分で覚える必要がありません。賢く活用して、あなたのアカウントのセキュリティをしっかり強化しましょう。

トピック CHECK!

「パスワード管理アプリ」でパスワードを安全に管理しよう

パスワード管理アプリは、大きく分けて次の3種類に分類できます。
それぞれの特長を理解し、自分に合ったものを選びましょう。

主な特長	代表例・使い方のポイント	注意点
スマホやPCのOSに内蔵されたタイプ		
スマホやPCの標準機能として利用でき、端末のアカウントと連動して動作します。	iPhone／iPadでは「パスワード」アプリ（iCloudキーチェーン機能）、Androidでは「Google パスワード マネージャー」が利用可能です。 端末によっては指紋認証や顔認証による自動入力にも対応しています。	OSをまたいだ利用には対応していない場合があります。 （例：iPhone ⇄ Windows、Android ⇄ macOSなど）
ブラウザに内蔵されたタイプ		
Webブラウザにパスワードを保存し、自動入力できます。	Google Chrome、Safari、Microsoft Edgeといった主なWebブラウザには、パスワードを保存したり、自動入力したりする機能が備わっています。 ブラウザの同期機能を利用すれば、別の端末や異なるOSでも共通で使えます。	近年は、より安全な認証方式である「パスキー」に対応する動きが進んでいるため、設定内容やセキュリティ機能を定期的に確認しましょう。
専用のパスワード管理サービスやアプリ		
パスワード管理に特化したサービスやアプリで、暗号化保存や安全な共有、漏洩チェックなどの機能が豊富です。	代表的なサービスとして、1Password（ワンパスワード）、Bitwarden（ビットウォーデン）、NordPass（ノードパス）などがあります。 ※上記は一例であり、特定のサービスの利用を推奨するものではありません。	利用にあたっては、各提供者の利用条件や搭載機能・各種設定を必ずご確認ください。 有料のものも多く、設定やバックアップの管理には少し慣れが必要です。

パスワード管理アプリでできること

パスワード管理ツールを使うと、主に次のようなことができます。
安心・安全かつ効果的にパスワードを管理しましょう。

パスワードをまとめて管理

- **パスワードの一元管理と安全な保存**
  複数のサービスのID・パスワードを暗号化して安全に一括管理。
- **強力なパスワードの自動生成**
  推測されにくく、十分に長いパスワードを自動生成し、セキュリティを強化。
- **パスワードの自動入力**
  ログイン画面でIDとパスワードを自動入力し、入力ミスや手間を削減。

どの端末からでも安全に利用

- **複数デバイスでの同期**
  スマホ、タブレット、PCなど、複数の端末間で安全にパスワード情報を同期。
- **多要素認証（MFA）との連携**
  ワンタイムパスワードの生成や、他の認証ツールとの連携により、セキュリティをさらに強化。
  ➡「多要素認証」については25ページもCHECK!

パスワードの安全性を評価・監視

- **パスワードの強度チェック**
  脆弱なパスワードを使っていないか検出し、強いパスワードへの改善を提案。
- **パスワードの漏洩チェック（ダークウェブ※監視）**
  過去の情報漏洩事案で自分のパスワードが流出していないか監視し、漏洩が確認された場合には警告。

※「ダークウェブ」とは、情報の売買といった不正な目的で使われることもある、検索エンジンでは見つからない匿名性の高いネット空間のことです。

大切な情報を安全に管理・共有

- **パスワード以外の情報の管理**
  クレジットカードや銀行口座、住所など、パスワード以外の機密情報も安全に保管。
- **安全なパスワード共有**
  家族や、所属組織のチームメンバーと、特定のパスワードを安全に共有。
- **緊急アクセス機能**
  万が一のことがあった場合に、信頼できる人にアクセス権を与える。

POINT 2

顔認証や指紋認証を積極的に使おう

パスワードを「作る・覚える・管理する」という手間を省き、なおかつ安全性を高める方法として「生体認証」があります。

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不可能に近く、非常に高いセキュリティを保つことができます。

最近のアプリやサービスは、生体認証機能があるスマホやPCで使用する場合、顔認証や指紋認証でログインできるように設定が可能です。設定手順も簡単で、まずはスマホやPCにあなたの顔や指紋を登録し、利用したいサービスやアプリ側で生体認証を使ってログインする設定を有効にしておくだけです。ぜひ積極的に活用しましょう。

トピック CHECK!

「多要素認証」ってなに？

「多要素認証（MFA：Multi-Factor Authentication）」とは、パスワードなどの認証情報に加えて、複数の要素を組み合わせることで不正ログインを防ぐ仕組みです。
1つの要素だけでは、パスワードの漏洩や端末の紛失などによって攻撃者に突破されるおそれがありますが、下記のような異なる種類の要素を組み合わせておくことで、攻撃者はすべてを同時に破ることが極めて困難になります。
こうした効果から、近年は多くのオンラインサービスで多要素認証が強く推奨されているため、自分が使っているサービスで多要素認証の設定が有効化されているかを確認しましょう。

知識情報（知っているもの：Something you know）

特長　本人しか知らない情報のことで、もっとも基本的な認証要素です。

代表的な例　パスワード、PINコード

所持情報（持っているもの：Something you have）

特長　本人が所有しているスマホやハードウェアトークンなど、別の機器を使うことでセキュリティを高めます。

代表的な例　SMSで確認コードが届くスマホ、一時的なコードを生成するアプリ（例：Google Authenticator）、USBやNFC※で接続した後にボタンを押して認証する専用デバイス（例：YubiKey）

※NFC＝スマホなどをかざして通信する近距離無線技術

生体情報（本人そのもの：Something you are）

特長　顔や指紋など、本人の生体情報を使って確認します。
利便性が高く、なりすましが困難です。

代表的な例　生体認証（例：顔認証、指紋認証、虹彩認証）
➡端末のロックを解除する際にも使用しますが、その端末でサービスにログインする際にも認証方法として利用できます。

コラム

WARNING!

パスワード漏洩の怖い話

あなたの大切なパスワードは、一体どこから盗まれ、
どのように悪用されてしまうのでしょうか？
主な手口を知り、しっかり対策しましょう！

手口その1 巧妙な「フィッシング詐欺」

フィッシング詐欺は、攻撃者が銀行や行政機関といった多くの人が日常的によく使う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です。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。

本当に起こり得る怖い話

ある日、茂礼手課長のもとに、いつも利用しているオンラインバンキングからメールが届きました。
「あなたの口座はアカウント認証に失敗しています。すぐに再ログインしてください」と書かれており、給与日やクレジットカードの引き落とし日が近かったため、焦った課長はすぐにリンクをクリック。表示されたのは、見慣れたログイン画面だったので、課長は何も疑わずにログインIDとパスワードを入力し、さらに口座番号や暗証番号まで入力してしまいました。
数日後、銀行から「不審な送金があった」との連絡があり、あの時アクセスしたサイトが実は偽のフィッシングサイトだったことを知り、課長は愕然としました。

どうすれば防げる？

最近のフィッシング詐欺は、本物と見分けがつかないほど巧妙になっており、一見して「怪しい」と気づくのは至難の業です。だからこそ大切なのが、「届いたメールやメッセージのリンクを安易にクリックしない」「誘導や催促するメッセージは疑う」という習慣です。
どんなに緊急に見えても、不安を感じても、まずはひと呼吸おいて立ち止まりましょう。
アカウントにアクセスしたいときは、メールやメッセージのリンクからではなく、いつも使っている公式サイトや公式アプリから直接アクセスするのが安全です。本当に緊急の連絡であれば、公式サイトやアプリ内にも同じ案内が掲載されているはずです。
この“ひと手間”が、あなたを詐欺から守ります。

➡ フィッシング詐欺への注意については、9ページや12・13ページも確認してにゃ！

手口その2 情報流出で「芋づる式」に危険が拡大！

あなたが使っているサービスの提供元がサイバー攻撃を受け、そこに登録していたパスワードを含む情報が流出してしまう、というケースも起こり得ます。このような情報漏洩があった場合、あなたがパスワードを他のサービスでも使い回していると、「芋づる式」にさまざまなサービスのアカウントが危険にさらされてしまいます。

本当に起こり得る怖い話

布施木さんは、ある大手通販サービスをよく利用していました。
ある日、その通販サービスから「大規模な不正アクセスにより、お客様のパスワードが流出した可能性があります」というお知らせが届きました。彼女はすぐに通販サービスのパスワードを変更しましたが、実はSNSでも同じパスワードを使っていたのです。
数日後、友人から「変なメッセージが届いているんだけど、アカウントが乗っ取られているのでは？」と連絡が。流出したパスワードが悪用され、攻撃者が布施木さんのSNSアカウントに不正ログインしていたのです。

どうすれば防げる？

異なるサービスで同じパスワードを使い回さないことが何より重要です。万が一、あるパスワードが流出してしまっても、同じものを他のサービスに使いまわしていなければ、被害拡大を防ぐことができます。
また、パスワード管理アプリを活用すれば、複雑なパスワードを一つひとつ覚えておく必要がなくなり、サービスごとに異なるパスワードを自動で生成・入力してくれるため、パスワードの使い回しを防ぎながら快適にさまざまなサービスを利用できます。
さらに、多要素認証を設定しておけば、不正ログインのリスクを大きく減らすことができます。

➡ パスワード管理ツールや他要素認証については、22ページも確認してにゃ！

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！

あなたのスマホや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。スマホやPCの設定画面に「システムアップデートのお知らせ」が表示されたら、すぐにインストールを進めましょう。

そうすることで、あなたのスマホやPC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となり、しっかり守られます。アップデートは後回しにせず、常に最新の状態を保つことが大切です。

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。

LINEのようなメッセージアプリや、Google Chrome・Microsoft Edge・Safariといったwebブラウザはもちろん、地図アプリ、SNS、通販サービス、オンラインバンキングなど、あらゆるアプリに脆弱性が見つかる可能性があります。

特にインターネット閲覧の入り口となるwebブラウザは、毎日使うだけに攻撃者に狙われやすいものです。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リスクもあります。

アプリの脆弱性も、最新のアップデートを適用することで修正されます。通知が来たら後回しにせず、OSと同じように、すぐにアップデートしましょう。

POINT 3

「自動アップデート」が断然おすすめ！

OSやアプリのアップデートを、毎回通知がくるたびに自分で対応するのは大変です。そこで「自動アップデート」機能をオンにしておきましょう。

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。

もしパケット（データ通信量）を気にしてオフにしている場合は、設定で「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ます。

あなたのスマホやPCの設定を確認し、OSやアプリの自動アップデート、Wi-Fi接続時の自動アップデートが有効になっているかチェックしてみましょう。

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が安心です。

非公式なサイトや不審なリンクからアプリをダウンロードすると、偽物や詐欺目的のアプリが紛れ込んでいる可能性があります。見た目は問題なさそうでもウイルスが仕込まれていて、知らない間にスマホやPCが感染してしまうリスクがあるため、注意が必要です。
また、人気アプリにそっくりな偽物が出回っていたり、アプリ名で検索をしたときに、怪しいダウンロードサイトが上位に表示されることもあるので、提供元が公式であるかをしっかりと確認しましょう。

いまの機種、いつまで使い続ける？スマホやPCの買い替えどきって？

スマホやPCを使っていて「なんだか最近、調子が悪いな…」と感じてきたら、端末の買い替えを検討するタイミングかもしれません。端末の寿命や性能の低下には、いくつかのサインがあります。安全で快適なデジタルライフを続けるために、買い替えの目安を知っておきましょう。
以下のようなサインを見逃さず、適切なタイミングでスマホやPCを買い替えることで、快適さだけでなく、セキュリティ面でも安心・安全な環境を保つことができます。
あなたのスマホやPCの「声」に耳を傾けて、必要に応じて新しい機種に切り替えましょう。

こんなサインがあったら、買い替えどき！

「サポートが終了」したら

使用しているOSやアプリの提供元からのサポートが終了している場合も、買い替えを検討するタイミングです。サポートが終了すると、脆弱性を修正するアップデートが提供されなくなり、リスクが高まります。特に、新バージョンのOSに端末が対応できなくなったら、買い替えを検討するタイミングです。

「動作が遅い」と感じたら

アプリがなかなか起動しなかったり、全体的に動作が遅くなったりしてきたら、買い替えを検討するタイミングです。特に、最新のOSやアプリをインストールしても改善しない場合は、ハードウェア（スマホやPC本体の能力）の限界が近づいている可能性があります。

「勝手に再起動」が増えたら

頻繁にフリーズしたり、突然電源が落ちてしまったりして、再起動が必要になるケースが増えてきたら、ハードウェアの劣化や不具合のサインです。

「バッテリーの減りがはやい」と感じたら

バッテリーは消耗品なので劣化は避けられません。充電したばかりなのに、すぐにバッテリー残量が減ってしまう場合、バッテリー交換が難しいようなら、端末の買い替えを検討しましょう。

「新しい機能が使えない」ことが増えたら

最新のアプリやサービスが動かない、使いたい機能に対応していない場合も、買い替えを検討すべきです。新しい機種は最新技術や機能に対応しており、より快適にさまざまなサービスや機能を利用できます。

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。

ログイン時の認証方法として、生体認証（顔認証や指紋認証）や多要素認証などの設定ができるときは、積極的に活用しましょう。これらは、パスワード単独よりも格段にセキュリティが高まります。

特に、初期パスワードが設定されている場合は、必ず変更しましょう。パスワードを変更する場合は、推測されにくく、十分に長い、また他サービスで使用していない強力なパスワードを設定することが重要です。

POINT 2

アクセス権限と情報の公開範囲を見直そう

新しいアプリやサービスを使い始めるとき、あなたのスマホやPCからさまざまな情報へのアクセスを求められますが、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。

例えば、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）など、アプリから要求されるアクセス権限が本当に必要かを一つずつ確認し、不要な権限はすべて無効にします。
また、プロフィールや連絡先などの、個人情報の「公開範囲」も重要なチェックポイントです。初期設定では公開とされている場合が多いため、サービスの利用目的をよく考え、必要以上に広範囲に情報が公開されていないかを確認しましょう。

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。

アプリによっては、初回起動時に何度も許可を求めてきたり、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があります。位置情報へのアクセスを求められたら、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」に限定しましょう。これは、バッテリーの消費削減にもつながります。
また、写真や投稿に位置情報が含まれたまま共有される場合もあるので、カメラやSNSの設定も確認しましょう。なお、設定をしていなくても、投稿内容から位置情報が特定されることもあるため、内容はもちろん、写真や動画を共有するときにも注意が必要です。

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。例えば、個人用クラウドへのデータ保存、未承認アプリの利用、私物PCやUSBメモリでのデータ取り扱いなどがこれにあたります。

「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

ちょっとした行動が、大きな漏洩につながるにゃ…
迷ったら一人で判断せず、上司やIT部門にまず相談、正しいツールの選定・利用で、みんなの安全を守ろう！

➡ 生成AI利用の注意点については、50ページも確認してにゃ！

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。

「誰にも見られていない」は大きな誤解！
多くの企業では情報を守るため、PC操作履歴や通信ログ、メール記録、ファイルアクセス履歴、入退室記録など、さまざまなログが管理されています。これらの記録から普段と違う行動パターンが検出され、不正が発覚するケースは多く、“見られていないように思える行動”でも、実際にはログから特定されています。

信頼を守る組織文化が大切！
セキュリティはシステムだけでなく、信頼し合える組織文化に支えられています。倫理観のあるオープンな職場づくりは、内部不正の強い抑止力になります。ルールは「会社のため」のみならず、あなたや周囲の人を守るためのもの。一時の油断が取り返しのつかない事態を招かぬよう、正しい行動を積み重ねましょう。

習慣 6

スマホやPCの紛失・盗難対策をしよう

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」

あなたのスマホやPCを守る最初の防御策は、画面ロック機能です。

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。画面ロックを解除するにはパスワードや生体認証（顔認証や指紋認証）、パスコード、PINコードなどの認証が必要になるように設定します。

生体認証は、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。

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。

画面ロックは、あなたの端末を守る大切な「扉」になります。

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。

まず､端末の｢位置情報サービス｣と｢検索機能｣をオンにしておきましょう。

- iPhoneやMacなら「探す」機能。iCloudのWebサイトから位置情報を確認できます。
- Androidなら「デバイスを探す」機能。専用アプリやWebサイトから位置情報を確認できます。
- 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ます。

次に、「リモートロック」と「データ消去」も設定しておきましょう。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、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ます。

POINT 3

公共の場での「覗き見」と「情報漏洩」に注意！

プライベートはもちろん、テレワーク／ハイブリッドワークが浸透したことで、さまざまな場所で仕事をすることも増えています。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。

まず、端末は常に手元に置き、無防備に放置しないようにします。覗き見防止フィルムを貼ることで、他人から画面を見られるリスクを減らせます。パスワードを入力するときは、周囲に人がいないか確認し、見えにくい角度で入力すること。

また、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ようにします。

さらに、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してみましょう。

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

万が一の事態に備えて、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」と、データを復旧できるようにするための「定期的なバックアップ」を設定しておくことも重要です。

まず、データを暗号化しておきましょう。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いますが、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。

次に、システム設定にあるバックアップ機能を有効するか、Google Drive、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りましょう。これにより、端末を紛失や破損してもデータを失うリスクを減らせます。

「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。

会社によっては機密保護の観点から、外部で作業してよい内容や場所、作業そのものを制限している場合もあるにゃ。外出先で業務を行う際は、必ず職場のルールに従おう！

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！

「もしかしたら詐欺に遭ったかも…。でも確信もないし、誰に相談したらいいか分からない…」そんなときは、一人で悩まず、警察相談ダイヤル「#9110（シャープ・イチ・イチ・マル）」へ相談してください。

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。もちろん、サイバー犯罪に関する相談にも対応してくれるので、セキュリティにおいても警察は心強い味方です。

もちろん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」へ電話しましょう。

こんなサインがあったら要注意！

次のようなサインは、あなたのスマホやPCが危険にさらされ、あなたの身に危険が迫っている兆候かもしれません。「これってどうなの？」と感じたら、すぐに専門家や信頼できる人に相談することが何よりも重要です。早めの行動が、大きな被害を防ぐことにつながります。

「にゃ？」って思うことがあったら、早めに相談するのがいちばんやで。
小さな違和感が、大きな被害を防ぐきっかけになるにゃ！

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。

警察庁「サイバー事案に関する相談窓口」
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。

MEMO

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、あなたの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。

「あれ？」と思ってほしいシチュエーションは、例えば下記のようなものです。
一つでも当てはまるものがあれば、迷わず確認・相談しましょう。

メッセージやアカウントまわりの異変

☑ **不審なメールやメッセージ**
・身に覚えのない送信元から、怪しいリンクや添付ファイル付きのメールが届く。
・知っている人からのメッセージでも、口調や内容に違和感がある。

☑ **身に覚えのないアカウント活動**
・利用していないサービスからログインやパスワード変更の通知が届く。
・パスワードが勝手に変更されてログインできない、アカウントがロックされている。
・自分のSNSやメールアカウントから、勝手に投稿・メッセージが送信されている。

PCやスマホの動作の異変

☑ **不審なアプリの起動**
知らないプログラムが自動的に起動したり、バックグラウンドで動いている。

☑ **ブラウザの異常**
・いつも見ているWebサイトや検索エンジンが、知らないものに勝手に変わっている。
・見覚えのない不審なツールバーや拡張機能が追加されている。

☑ **ファイルやデータの異変**
・ファイルが突然消えたり、内容が勝手に書き換えられている。
・身に覚えのないファイルやフォルダが作成されている。
・データが閲覧できなくなっている。（暗号化されている。）
・データと引き換えに身代金を要求するメッセージが表示される。

金銭がらみ・警告の表示

☑ **不審な請求や取引**
クレジットカードや銀行口座、電子マネーなどに、身に覚えのない利用履歴や請求が発生している。

☑ **怪しいポップアップや警告**
突然、不審なポップアップが表示され、ウイルス感染やシステムエラーを警告したり、サポートへの問い合わせや怪しいソフトウェアのインストールを促される。

☑ **セキュリティソフトの警告**
利用しているアンチウイルス（ウイルス対策ソフト）が、ウイルスを検出したとアラートを上げている。

巻末コラム

生成AIの光と影

近年、ChatGPTに代表される生成AIは驚くべき速さで進化し、文章や画像の生成、要約、アイデア出しなど、創作から業務支援まで幅広い場面で活用され始めています。その能力は私たちの働き方にも大きな変化をもたらし、今やAIは「未来の技術」ではなく、「身近なパートナー」と言える存在になりつつあります。

しかし、その“光”の部分だけに目を向けるのは危険です。情報が意図せずAIの学習に利用されてしまったり、AIが生成した精巧な偽情報が拡散したりといったリスクも存在します。また、ときに他者の著作権・肖像権の侵害につながる事案や、攻撃者が生成AIを悪用して巧妙な詐欺メールや攻撃コードを作るといったケースも報告されています。

生成AIに関する主なセキュリティリスク

☑ 機密情報の漏洩
入力した情報がAIの学習に利用され、意図せず外部に提供される可能性がある。

☑ 誤情報・偽情報（フェイク）の生成と拡散
AIが事実に基づかない情報や画像・動画を生成し、誤解や混乱を招く。

☑ 著作権・肖像権侵害
学習データや生成物が権利保護された内容と類似し、侵害にあたる場合がある。

☑ 悪意ある利用（攻撃・詐欺への悪用）
AIが自然な文章やコードを生成できるため、フィッシングメールやマルウェア作成に悪用される。

☑ セキュリティ脆弱性
AIモデルや、AIを組み込んだシステムに新たな脆弱性が発見されるほか、AIが生成したコードに脆弱性が含まれるケースもある。

これからの社会で生成AIと上手に付き合うためには、メリットとリスクを正しく理解し、適切な使い方を身につける必要があります。個人としてはAIに入力する情報に注意を払い、AIの回答内容は鵜呑みにせず、事実確認する姿勢が欠かせません。組織としてはガイドラインの整備や教育を行い、従業員が安心してAIを活用できる環境を作ることが求められます。

生成AIは“諸刃の剣”と言われてるけど、正しく使えば、生産性も安全性もちゃんと高められるにゃ！

生成AIを安全に使いこなすためには、
個人でも組織でも、いくつか押さえておきたいポイントがあります。
以下の対策を参考に、適切な利用を心がけましょう。

個人の対策

サービス選定は慎重に

・利用する生成AIサービスのプライバシーポリシーや利用規約を確認する。
・信頼できる提供元のサービスを選ぶ。

入力は慎重に

・個人情報や機密情報は入力しない原則を徹底する。
・業務で利用する場合は、会社のガイドラインを必ず確認する。

AIの回答を鵜呑みにしない

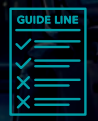
・AIが生成した内容はそのまま使用せず、必ず人が事実確認をする。
・重要な意思決定に用いる場合は、複数の情報源や専門家の判断を参照する。

最新情報をキャッチアップ

生成AIの技術やリスクは日々進化するため、常に最新の情報を得るよう努める。

組織の対策

利用ガイドラインの策定



利用範囲、入力してよい情報・禁止情報、生成物の取り扱いといったルールを明確に定める。

セキュリティ教育の実施

従業員に対し、リスク認識と安全な利用方法に関する定期的な教育を実施する。

適切なツールの導入・検討

・業務利用に耐えうる生成AIサービス（プライベートAIやオンプレミス型など）を検討する。
・安全に業務利用できるよう、必要に応じてセキュリティ機能や管理ツールと組み合わせて運用する。

責任体制の明確化

生成AI利用における責任の所在を明確にし、利用ガイドライン・ルールを社内で共有し、守られているか確認する。

シーン別 理解を深める

20の事例とQ&A

こんなことよくあるよね？

身近な手口を知ろう編

事 例

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、「フィッシング詐欺」の可能性があります。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ようにしましょう。

解　説

最近の詐欺は、“思わぬ得をする”甘い誘い方が増えています。例えば「ポイントバックがあります」「アンケート回答でギフト券プレゼント！」といった魅力的な誘いがメッセージで届きます。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。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。このようなメッセージを受け取った場合は、公式サイトや公式アプリで情報の正誤を確認するか、不安な場合は何もせずメッセージを削除しましょう。

詐欺への注意や見分け方については「習慣１：誘導や催促のメッセージを警戒し、確認しよう」（８ページ～）の内容も参考にしてください。

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。

事 例

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」の典型的な手口であり、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。
このようなとき、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し、「×（閉じる）」ボタンで表示を閉じられるか試してみましょう。閉じられない場合はPCを強制終了し、再起動しましょう。

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。このような表示が出た場合は、ポップアップの内容は無視し、推奨されている方法で警告画面を閉じましょう。

詐欺への注意や見分け方については「習慣１：誘導や催促のメッセージを警戒し、確認しよう」（８ページ～）の内容も参考にしてください。

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。

事 例

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。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りましょう。

解　説

「なりすまし」では、家族や友人、上司や取引先、行政機関など、信頼できる人を装い、情報や金銭をだまし取ったり、攻撃を仕掛けたりする手口が典型的です。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。いつもと様子が異なる場合は本人に確認し、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相談しましょう。

詐欺への注意や見分け方については「習慣１：誘導や催促のメッセージを警戒し、確認しよう」（８ページ～）の内容も参考にしてください。

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…。

事 例

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。まずは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しましょう。

解　説

宅配業者をはじめ、銀行や税務署など、信頼できるサービスや機関を装って情報を入力させようとするのは「フィッシング詐欺」の常套手口です。メッセージのリンクはクリックせず、公式サイトや公式アプリを利用して、サービスからの通知を直接確認しましょう。

ほかにも、「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。

詐欺への注意や見分け方については「習慣１：誘導や催促のメッセージを警戒し、確認しよう」（８ページ～）の内容も参考にしてください。

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。

事 例

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。安易にQRコードからアクセスせず、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みましょう。

解　説

昨今、QRコードを悪用した詐欺手口が確認されています。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。とても便利で、さまざまな場面で見かけるQRコードですが、安易に読み取らないようにしましょう。

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！

シーン別 理解を深める

20の事例とQ&A

こんなことやりがちだよね？

見落としがち な設定編

事 例

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。
このような被害を防ぐには、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、管理することが有効です。さらに、生体認証や多要素認証も設定しておくことで、万が一、パスワードが漏洩しても不正ログインされるリスクは大幅に低減できます。

パスワード設定の注意や安全な管理方法については「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」（20ページ～）の内容も参考にしてください。

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！
ここが乗っ取られると一網打尽にされてしまうので、強いパスワードと多要素認証でしっかり守ろうな！
パスワードが漏洩するとどんなに怖いか、コラム（26～27ページ）も読んでにゃ。

事 例

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うため、必ず設定するようにしましょう。

解　説

「多要素認証」は、パスワードなどの認証情報に加え、複数の要素を組み合わせることで強力な防御力を発揮します。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。面倒に感じても、サービス利用開始時や、セキュリティ機能の追加案内があればすぐに設定を完了させましょう。

多要素認証については「多要素認証ってなに？」（25ページ）の内容も参考にしてください。

…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！

事 例

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

管理者アカウントはシステム全体の設定やユーザー管理に影響するため、不正利用されると重大事故につながります。

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。

退職や異動時には速やかにアカウントを無効化・削除し、不要な権限を残さないことが重要です。

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！

事 例

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。極端に恐れる必要はありませんが、位置情報や友人のタグ付け、公開範囲など、設定をしっかり確認し、安全に楽しみましょう。

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。

こうしたトラブルを防ぐためには、公開範囲やタグ付けなどの設定を事前に確認することが欠かせません。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き、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ましょう。

設定については「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」（34ページ～）の内容も参考にしてください。

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。

事 例

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。アップデートの通知は必ず受け取るようにし、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ましょう。

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。ソフトウェアの提供元は脆弱性修正のためのアップデートを配布しているため、通知が出たら後回しにせず、速やかに更新して最新の安全な状態を保つことが重要です。

アップデートの重要性については「習慣4：OSやアプリを最新状態にアップデートしよう」（28ページ～）の内容も参考にしてください。

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。

事 例

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するため、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にアップデートしましょう。

解　説

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。
なお、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、買い替えも必要となります。

スマホやPCの買い替えどきについては、「コラム」（33ページ）の内容も参考にしてください。

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…。

シーン別 理解を深める

20の事例とQ&A

これぐらいなら大丈夫！ と思いがち
モラル＆ポリシーを守ろう編

事 例

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。誰に見られる可能性があるかを意識して慎重に判断しましょう。

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。「発信したい気持ち」と「守らなければならない情報」を切り分け、会社ルールや社会的モラルに従い、投稿前に内容を確認しましょう。

発信する情報の取り扱いについては「習慣２：投稿が誰から見られているか意識しよう」（14ページ）の内容も参考にしてください。

「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！

事 例

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。社外での作業が認められている場合でも、プライバシーフィルターやカバーなどのツールを活用したり、背後に人が立たない席に座る、周囲に注意を払うといった工夫や意識で対策しましょう。

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があります。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など、複数の対策を組み合わせると効果的です。さらに、会社によっては機密保護の観点から、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、必ず職場のルールも確認しましょう。

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！
ショルダーハック対策は、コラム（45ページ）も見てにゃ。

事 例

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。
会社のセキュリティ方針やルールに従い、指定された業務USBメモリや業務用クラウドストレージを利用してデータの保存・共有を行いましょう。

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。面倒でも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・共有しましょう。会社が管理する業務用USBメモリやクラウドストレージには暗号化やアクセス制限などのセキュリティ対策が施されており、安心して利用できます。

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やで！
シャドーITの危険性や注意は、コラム（38ページ）も読んでにゃ。

事 例

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。
必ず行政やメディアなどの公式発表の内容を確認しましょう。

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。流れてきた情報は鵜呑みにせず、信頼できる情報源で情報日付や内容の確認を取るひと手間が必要です。根拠不明な情報を広めたり、デマに加担したりしてはいけません。「いま必要な正しい情報か」を見極めて行動しましょう。

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。

事 例

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。甘い誘いの言葉や報酬に惑わされず、速やかに上司や社内の情報システム担当者へ報告し、関わらないようにしましょう。

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。甘い誘いには乗らず、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しましょう。そして何より、甘い誘いには乗らないという強い意志を持つことが重要です。

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。
不正行為の危険性や注意は、コラム（38ページ）も読んでにゃ。

シーン別 理解を深める

20の事例とQ&A

しまった！ の後が大事
対応力を身につけよう編

事 例

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 紛失モードを有効化し、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。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しましょう。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も行い、まずは第三者による悪用を阻止しましょう。

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。キャリアの探索サービスや、端末標準のデバイスを探す機能も有効です。長時間見つからない、海外や遠隔地での紛失・盗難の可能性が高い、電波が途絶え追跡が不可能といった「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します。なお、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ことも忘れないでください。

端末の紛失対策や紛失時の対応については「習慣６：スマホやPCの盗難・紛失対策をしよう」（40ページ～）の内容も参考にしてください。

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。

事 例

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。自己判断・自己解決で終わらせず、しかるべき窓口と連携して、情報流出を防ぐための適切な措置を迅速にとりましょう。

解　説

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することが大切です。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、状況に応じて適切な措置を取りましょう。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。個人で判断せず、組織として責任を持って迅速に対応し、再発防止につなげましょう。

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な。

事 例

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

不審メールは自己判断・自己解決で終わらせず、社内ルールに従って上司や情報システム担当者に報告しましょう。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、組織全体で情報共有し対応することで、被害拡大を未然に防ぐ重要な対策になります。

解　説

不審メールを見つけても削除して終わりではなく、社内で定められた報告フローを確認し、速やかに報告しましょう。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。

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。

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。迷いや不安があれば、自己判断せずに上司や情報システム担当者に相談することが大切です。

確認・相談すべきシチュエーションについては「習慣7：少しでもおかしいと思ったら、すぐに相談しよう」（46ページ～）も参考にしてください。

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。

事 例

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。問い合わせや支払いに応じてしまうと被害が拡大するため、無視して画面を閉じることが正しい対応です。

解　説

ワンクリック詐欺は、サイトを閲覧しただけで「会員登録が完了しました」「料金を支払ってください」などと表示し、利用者を焦らせて金銭をだまし取る典型的な手口です。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。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。画面は閉じて相手にせず、決して支払いをしないことが最も重要な対策です。

詐欺への注意や見分け方については「習慣１：誘導や催促のメッセージを警戒し、確認しよう」（８ページ～）の内容も参考にしてください。

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」に相談してな！
相談先はコラム（48ページ）に紹介しているにゃ。

監修者のご紹介

本書は、2016年発行の初版に引き続き、エムオーテックスが推進する共創型のセキュリティ啓発プロジェクト『NO MORE 情報漏洩 2050』に賛同いただいた有識者2名の監修のもと制作しています。未来の安全につながるセキュリティ知識を分かりやすく届けるため、セキュリティの第一線で活動する両氏とエムオーテックスは連携し、安心してデジタル技術を活用できる社会づくりを目指して取り組んでいます。

PROFILE

岡田 良太郎氏

OKADA RIOTARO

株式会社アスタリスク・リサーチ
代表取締役

今どきの脅威に対応することは決して容易ではありません。それに伴い、安全なビジネス環境を実現する技術や仕組みは大きく変化してきました。企業内外では、情報システムに関わる多くの組織的な努力が重ねられていることでしょう。

一方で、そうした仕組みを活用する「人」の側はどうでしょうか。私たちはネットのサービスやアプリをますます活用していますが、脅威も同時に変化していることを、どれほど意識しているでしょうか。残念ながら、難しい、ややこしい、めんどくさい——そう感じて、セキュリティを維持する行動から目を背けてしまう場面は少なくありません。

そこで本書は、セキュリティの仕組みや専門技術を解説するのではなく、この複雑な環境の中で働く一人ひとりが、無防備な状態から抜け出すための「行動の習慣」を示すハンドブックとして刷新しました。ここにあるのは、アップデートされた、今日から実践できる行動です。この一冊が、皆さん自身と周囲にいる仲間を守る助けとなることを願っています。どうか、ご安全に。

1968年生まれ、神戸市出身。神戸市立工業高等専門学校電気工学科卒業。ソフトウェアエンジニアを経て、2006年に株式会社アスタリスク・リサーチを創業。企業のセキュリティ実践支援事業を展開している。
公益活動としては、総務省実践的サイバー防御演習CYDER実行委員、ビジネスブレークスルー大学講師として、サイバーセキュリティを扱える人材の育成に従事。Hardening Projectオーガナイザ、OWASP Japanリーダーなどコミュニティ貢献を推進している。
2025年、兵庫県警サイバーセキュリティ対策アドバイザーに就任。MBAを保持。

PROFILE

徳丸 浩氏

TOKUMARU HIROSHI

EGセキュアソリューションズ株式会社
取締役CTO

2016年発行の旧版から約10年をおいて新版を世に出すことができました。当時から本書は、正確性と読みやすさの両立という点で画期的でしたが、新版ではその特徴を維持しつつ、最新のセキュリティ状況を踏まえて内容を大幅に見直しました。フィッシング対策、SNS投稿の配慮、パスワード管理、OS・アプリ更新、初期設定見直し、紛失対策、早期相談など、「なぜ必要か」と「どうすべきか」をセットで具体的に示しています。リスクをゼロにできなくても大幅に下げられる、そんなポイントが詰まった実践的な1冊です。

1985年京セラ株式会社に入社後、ソフトウェアの開発、企画に従事。1999年に携帯電話向け認証課金基盤の方式設計を担当したことをきっかけにWebアプリケーションのセキュリティに興味を持つ。2004年同分野を事業化。
2008年独立して、Webアプリケーションセキュリティを専門分野とするHASHコンサルティング株式会社（現EGセキュアソリューションズ株式会社）を設立。
脆弱性診断やコンサルティング業務のかたわら、ブログや勉強会などを通じてセキュリティの啓蒙活動をおこなっている。
2023年イー・ガーディアングループのCISOに就任。セキュリティレベル向上だけでなく、活動を通して得たノウハウをサービスやセミナーコンテンツにも還元し、広くセキュリティの啓蒙活動に邁進。

発行元：

エムオーテックス株式会社のご紹介

デジタルセキュリティの課題から、人と社会を解決する。

MOTEX

MOTEX（エムオーテックス）は、国産のセキュリティメーカーとして「LANSCOPE（ランスコープ）」ブランドのセキュリティプロダクト・サービスを展開し、「Secure Productivity（安全と生産性の両立）」をミッションに、企業・組織のサイバーセキュリティ課題の解決を支援しています。
1990年の創業以来、大阪本社を拠点に、お客様がエンドポイント（端末）・ネットワーク・クラウドサービスを安心して活用できるビジネス環境づくりに取り組んでいます。

サイバーセキュリティ任せるなラ、LANSCOPE（ランスコープ）

累計導入実績30,000社以上※1

- クラウドIT資産管理 市場シェア NO.1 ※2
- パブリッククラウド向け脆弱性診断 市場シェア NO.1 ※3
- ITreview 顧客評価 6部門 LEADER ※4

IT資産管理、情報漏洩対策、マルウェア対策といったエンドポイントセキュリティ機能に加え、総合的な診断・コンサルティングを通じ、お客様のサイバーセキュリティ課題の解決をトータルでご支援します。

Pick UP

経産省 SCS評価制度（セキュリティ対策評価制度）※5支援
各業界セキュリティガイドライン支援

ガイドライン対応サポートアカデミー

国や業界のセキュリティガイドラインへの対応が求められる中、MOTEXは「好きな時に、ずっと使える。学びとコンサルで築く確かなセキュリティ。」をコンセプトに、あらゆる企業・組織のセキュリティレベルの向上を「アカデミー形式」で支援するセキュリティコンサルティングパッケージを提供しています。
コンサルタントによる個別支援に加え、ポータルを活用した動画学習を通じて、体系的かつ効果的にセキュリティガイドラインの遵守を支援します。

※1　MOTEX調べ
※2　株式会社テクノ・システム・リサーチ「2025年版 エンドポイント管理市場のマーケティング分析」の「PC 資産・PC セキュリティSaaS市場 メーカー シェア 2024年 ブランド別市場シェア」分野
※3　ITR「ITR Market View:サイバー・セキュリティ・コンサルティング・サービス市場2024」パブリッククラウド向け脆弱性診断サービス／CSPMサービス市場：ベンダー別売上金額シェア（2024年度（予測））
※4　ITreview Grid Award 2025 Winter：統合運用管理ツール / MDM・EMMツール / IT 資産管理ツール / ログ管理システム / ウイルス対策ソフト / EDR
※5　「サプライチェーン強化に向けたセキュリティ対策評価制度」の略称（2025年12月に経済産業省が公表した「サプライチェーン強化に向けたセキュリティ対策評価制度 に関する制度構築方針（案）」より）

NO MORE 情報漏洩2050

「共創型」セキュリティ啓発プロジェクト

2050年の未来を守るホワイトハッカー「ラン」と、猫型ロボット「BANNYA」は、セキュリティ事故の多さに危機感を持ち、“意識改革は過去から！”と現代にタイムスリップ。『NO MORE 情報漏洩 2050』のナビゲーターとして活動中です。

共創しよう、私たちのセキュアな未来を。

『NO MORE 情報漏洩 2050』プロジェクトは、すべての人が安心してデジタル技術活用できるセキュアな社会の実現を目指す、共創型セキュリティ啓発プロジェクトです。

セキュリティを“自分ごと化”し、「文化」へ。

セキュリティで大切なことは、一人ひとりの意識です。
日々の小さな“気をつける”があなた自身を守る大きな力になります。
そのために、私たちはこの活動を通じて、まずはより多く人にセキュリティについて“知ってもらうこと”から始め、みんなで“一緒に考えていくこと”で、セキュリティの“自分ごと化”を促します。
さらに、こうした“取り組みを発信して広めること”で、セキュリティを「文化」として社会に根付かせることを目指します。

プロジェクトの取り組み

サイバーセキュリティハンドブック／セキュリティ教育コンテンツ

誰もが身につけておくべき「セキュリティ7つの習慣」が身に付くハンドブックと、それをもとにしたセキュリティ教育コンテンツを無償提供しています。

セキュリティ啓発エバンジェリスト

セキュリティの“自分ごと化”を使命に、SNS・イベント・セミナー、メディアなどを通じて、セキュリティの大切さを分かりやすく伝え、広め、一緒に考えていく“きっかけ”を届けていきます。

～共創プロジェクト～ NEO TOKYO PUNKS×NOMORE情報漏洩

NIKO24氏が率いるデジタルアートプロジェクト「NEO TOKYO PUNKS」と連携し、セキュリティ啓発を目的に、キャラクターなどのコンテンツを共創しています。

『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

イラストレーターのご紹介

エムオーテックスの共創型セキュリティ啓発プロジェクト『NO MORE 情報漏洩 2050』は、NIKO24氏が率いるデジタルアートプロジェクト「NEO　TOKYO　PUNKS」が掲げるコラボレーション型プロジェクト「Co-CREATE NEO TOKYO 2050」に参画し、セキュリティ啓発コンテンツを共創しています。
その一環として、本書の挿絵は NIKO24氏により制作されています。

茂礼手 太郎・布施木 ます子

LAN & BANNYA.

NEO TOKYO PUNKS

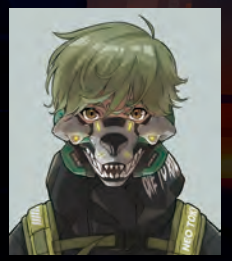
「NEO TOKYO PUNKS」および『Co-CREATE NEO TOKYO 2050』について：
「NEO TOKYO PUNKS（ネオトーキョーパンクス）」は、日本のイラストレーター・NIKO24氏が描いた横顔のイラストを特徴とするNFT（Non-Fungible Token）のコレクションで、サイバーパンクな世界観のもと、さまざまなガジェットを装着したキャラクターが描写されるデジタルアートです。近年はラッパーの呂布 カルマ氏やスケートボード日本代表の堀米　雄斗選手とのコラボレーションで注目されています。各キャラクターはランダムに各パーツを組み合わせる「ジェネラティブアート」と呼ばれる手法で作成されており、今後はNFTホルダー向けのイベントやメタバース上での3D展開も予定されるなど、日本発のエンターテインメント作品として、海外のNFTアートコレクターからも熱い視線が注がれています。

NEO TOKYO PUNKS 公式サイト　https://neotokyopunks.com/

Co-CREATE NEO TOKYO 2050

そして、『Co-CREATE NEO TOKYO 2050』は、NEO TOKYO PUNKSとさまざまな企業・自治体・教育機関などがコラボレーションし、2050年の東京・NEO TOKYOを「共創」していくプロジェクトです。「プロジェクトに関わる全ての人が主人公となって未来を想像し、誇らしく思える夢のある未来を共に創っていく」ことをテーマに、企業・組織が持つ技術と情熱をNTPというIP（Intellectual Property：知的財産）を使ってコンテンツ化し、世の中に発信する活動を展開しており、現在、山梨県やdocomo STARTUPなどが参加しています。

Co-CREATE NEO TOKYO 2050 公式サイト　https://neotokyo2050.com/



NIKO24
FOUNDER / CREATOR

MESSAGE

サイバーセキュリティと聞くと、小難しい印象を受けたり、「自分とは関係ない」と思いがちですよね。今回は「NEO TOKYO PUNKS」というIPを活用することで、「このクリエイティブいいな」「面白そう」と、少しでもセキュリティに興味を持って感じてもらえるよう描きました。楽しみながら意識を変えるきっかけを作れたら嬉しいです。日常の中で"セキュリティ"を考える一歩になればと思います。

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』

監修　岡田 良太郎（株式会社アスタリスク・リサーチ）
徳丸 浩（EG セキュアソリューションズ株式会社）

企画・編集　エムオーテックス株式会社『NO MORE 情報漏洩 2050』プロジェクト

制作　株式会社ファーストブランド

イラスト　NIKO24（NEO TOKYO PUNKS）

発行　エムオーテックス株式会社
〒532-0011 大阪市淀川区西中島 5-12-12
https://www.motex.co.jp/

印刷・製本　株式会社北斗社

・本書はセキュリティ啓発を目的とした非売品です。
・広くご活用いただくため、Amazonでも実費にてお求めいただけます。

◉ お問い合わせ先
エムオーテックス株式会社
『NO MORE 情報漏洩 2050』プロジェクト事務局
E-mail：press@motex.co.jp

※乱丁・落丁はお取り換えいたします。

M2602-001