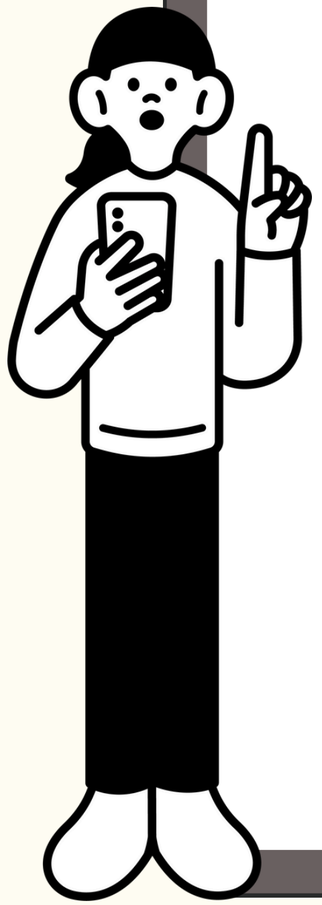
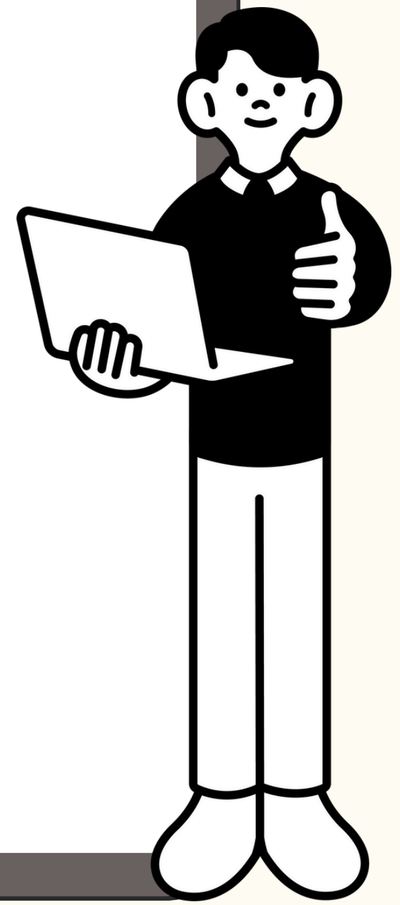


docomo Solutions

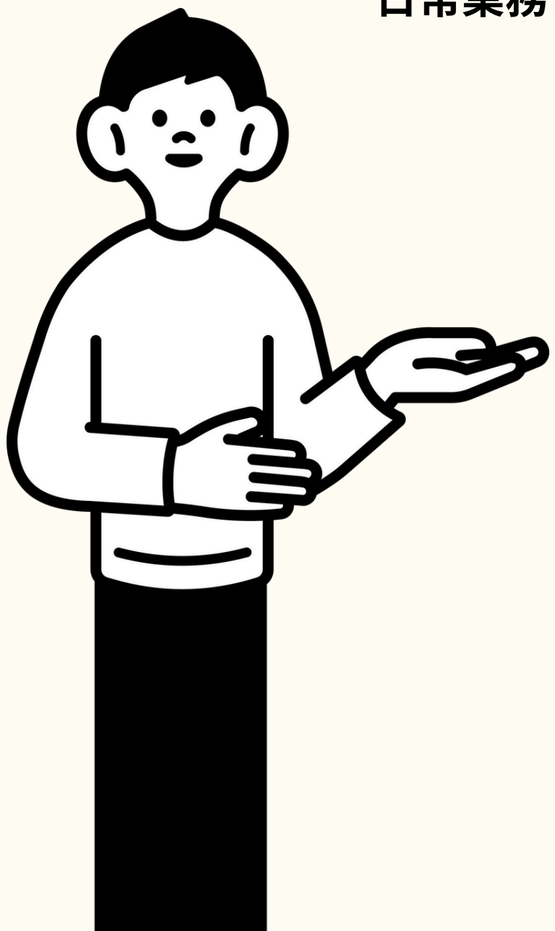
セキュリティ教育通信
2025年 12月号

NTTドコモソリューションズ株式会社



docomo Solutions

12月の
セキュリティ教育テーマ



日常業務で起こりやすい3つのセキュリティリスクについて、シンプルにわかりやすく学んでいきます。

1つ1つのテーマで『なぜ危ないのか』『どう防ぐか』を具体的に紹介していきます。

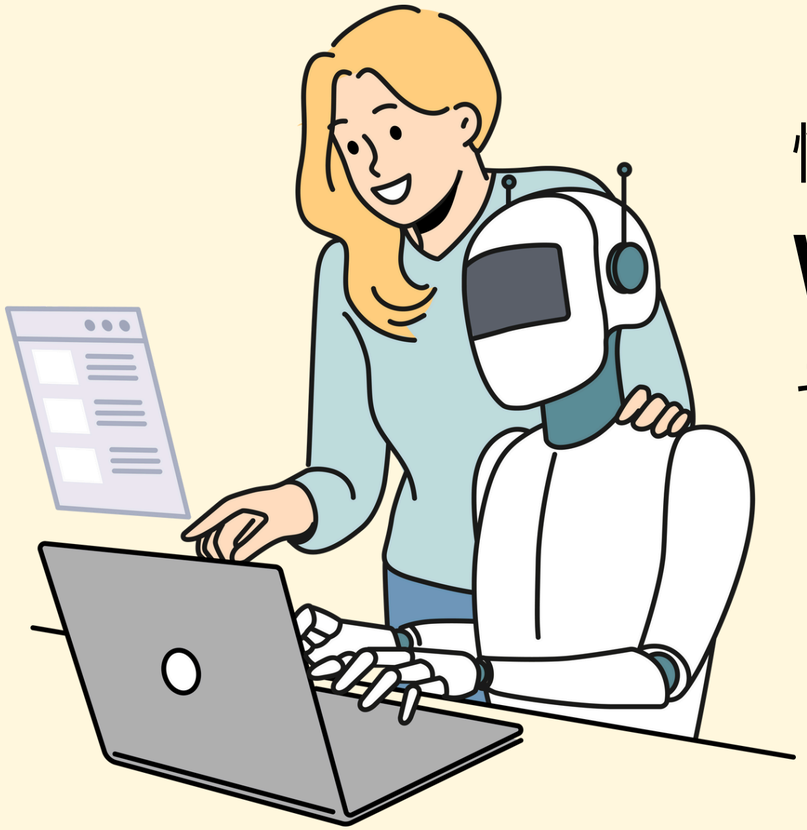
1 基本対策｜Basic Countermeasures
生成AIが紹介したサイト、本当に安全？

2 インターネットの脅威｜Online Threats
QRコードを悪用したフィッシング詐欺の増加

3 季節・社会動向の注意点｜Seasonal Security
年末年始に増える３つのセキュリティリスク

１．生成AIが紹介したサイト、本当に安全？

生成AIの言うこと、ぜんぶ信じてない？



情報の探し方が、

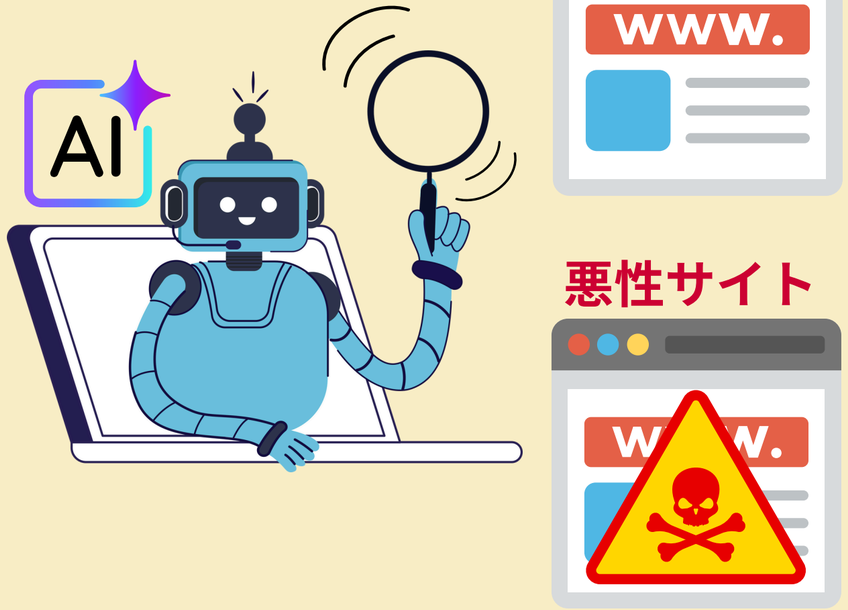
WEB検索 から **AI検索** に変わってきている今、

その便利さの裏にある**危険**を意識できていますか？

INNOVATING WITH AIの調査によると、ユーザーの約８割が、
「AI検索は従来の検索より効率的」と感じており、情報収集の“入口”が変わり始めています。

１．生成AIが紹介したサイト、本当に安全？

便利な生成AIの回答にも、“ 思わぬ落とし穴 ” が潜んでいます。



01 実は生成AIも完璧じゃないんです

生成AIは危険なサイトを除外するよう工夫されていますが、
完全ではありません。

02 生成AIが教えてくれた情報＝安全とは限りません

詐欺サイトや悪性サイトが、
生成AIの回答に混じることもあります。

03 だから、最後は自分の“確認力”です

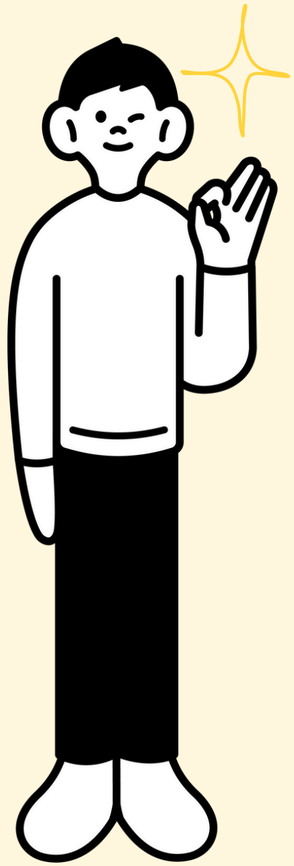
生成AIの提示を「安全」と思い込まず、
「本当に正規のサイトか？」を自分で確認しましょう。

生成AIはあなたの味方。でも、安全を守るのは “ あなた自身 ” です。

１．生成AIが紹介したサイト、本当に安全？

生成AIを正しく使うための理解度チェック！

内容	YES/NO
生成AIも完璧ではないと理解した	□ / □
生成AIが紹介した情報も確認が必要と理解した	□ / □
最後は自分の確認が大切だと理解した	□ / □



２．QRコードを悪用したフィッシング詐欺の増加

そのQRコード、本当に安全？

※本資料に掲載のQRコードは実在の詐欺サイトではなく、当社のサイトに遷移する安全なものです。

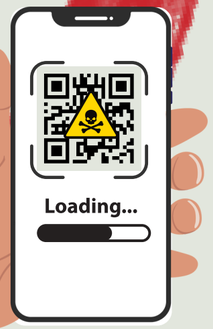
２．QRコードを悪用したフィッシング詐欺の増加

QRコードもURLリンクと同じ“攻撃の入口”！

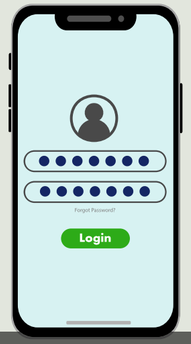
1 攻撃者はQRコードを含むスパムを送信します。

2 スパムメールなどを受信します。

その仕組みとは...



3 スマートフォンで
QRコードをスキャンします。



4 QRコードは攻撃者の作成した
フィッシングサイトにつながります。

5 そこでID/パスワードなどの
個人情報を入力してしまうと搾取されます。

２．QRコードを悪用したフィッシング詐欺の増加

なぜ今、QRコード詐欺 が増えているのか？

1 セキュリティの検知をすり抜ける構造にある

- メールにURLが表示されていないため、**メールセキュリティ検知を回避しやすい**
- 攻撃者は**業務PCのセキュリティ防御を避けるため、QRコードでスマホ端末へ誘導**する

2 思い込みを突かれる

- 「スマホで読み取るから安全」と思い込んでしまう
- 「公式っぽいから大丈夫」「QRコードだから安心」と思い込んでしまう

3 私用端末でアクセスしてしまう

- **会社PCではブロックされる攻撃も、私用スマホや社外端末だとセキュリティが甘い**
- 結果として、**企業のセキュリティ対策をすり抜けて被害に直結してしまう**

QRコード詐欺は「人の行動」を狙った攻撃です。
不審なメールなどのQRコードは読み取らないことを徹底しましょう！

２．QRコードを悪用したフィッシング詐欺の増加

QRコード詐欺にだまされないために

- □ 不審なQRコードは利用しない
- □ 業務ログインは会社端末から行う
- □ QRコードは「安全」と思い込まない
- □ 安易にIDやパスワードは入力せず、慎重に確認する

日常のちょっとした意識が、大きな被害を防ぎます。
便利さの裏にあるリスクを忘れず、一呼吸おきましょう。

季節・社会動向の注意点｜Seasonal Security

３．年末年始に増える３つのセキュリティリスク

2倍※ **この数字**

何の増加率だと思いますか？

※出典：デジタルデータソリューション／サイバーセキュリティクラウド 各社調査より（2022–2024）

NTT docomo Solutions

季節・社会動向の注意点｜Seasonal Security

３．年末年始に増える３つのセキュリティリスク

年末年始、サイバー攻撃や詐欺メールの件数は他の時期の**約２倍**に増えています。
背景には**「お金・忙しさ・油断」が重なる季節特有の行動パターン**があります。

セキュリティリスク		背景にある“人の動き”
① お金に関する“だましメッセージ”	**ボーナスやセール、宅配便・税金などを装った偽メールやSNSメッセージにだまされる**	年末は**「お得・支払い・振込」など お金が動く時期だから**
② 年末処理の“駆け込みミス”	**確認不足・誤送信・データ削除など、焦りからのヒューマンエラー**	**「年内に終わらせたい」「早く帰りたい」**という心理で確認が甘くなる
③ 端末の“うっかり放置”	**社用端末を家族や他人が触ってしまい、情報が閲覧される**	長期休暇前、**ロックや電源OFFなどの確認を後回しにしがち**

■対策・注意点

- ☑ 「ボーナス」「セール」「還付金」などの文言に注意し、冷静に確認。
- ☑ 今年最後の作業こそ、送信前にもう一度チェック。
- ☑ 休暇前は使わないPCの電源を落とし、鍵の付いた場所に保管するなどの対策を。

焦らず、慌てず、確認する。それだけで守れる情報がある。

３．年末年始に増える３つのセキュリティリスク

セキュリティリスクの理解度チェック！

内容	YES/NO
年末は金銭を狙う詐欺が増えると理解した	□ / □
焦りや確認不足がミスを招くと理解した	□ / □
休暇前は電源OFFと端末の管理の大事さを意識できた	□ / □