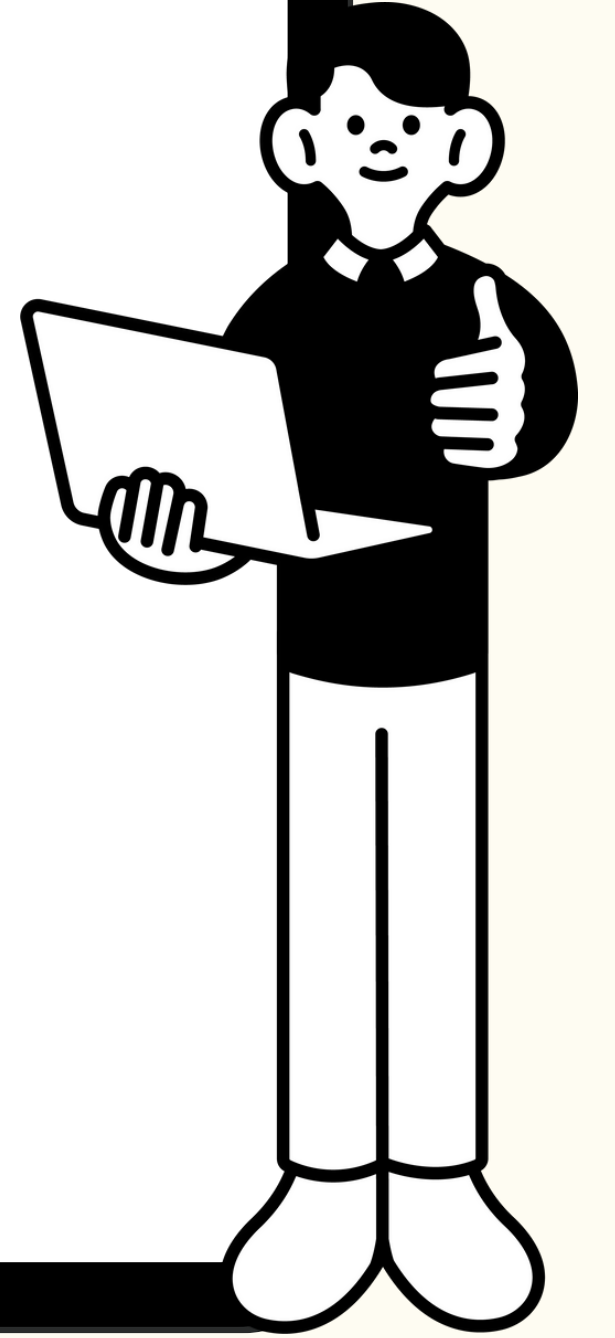
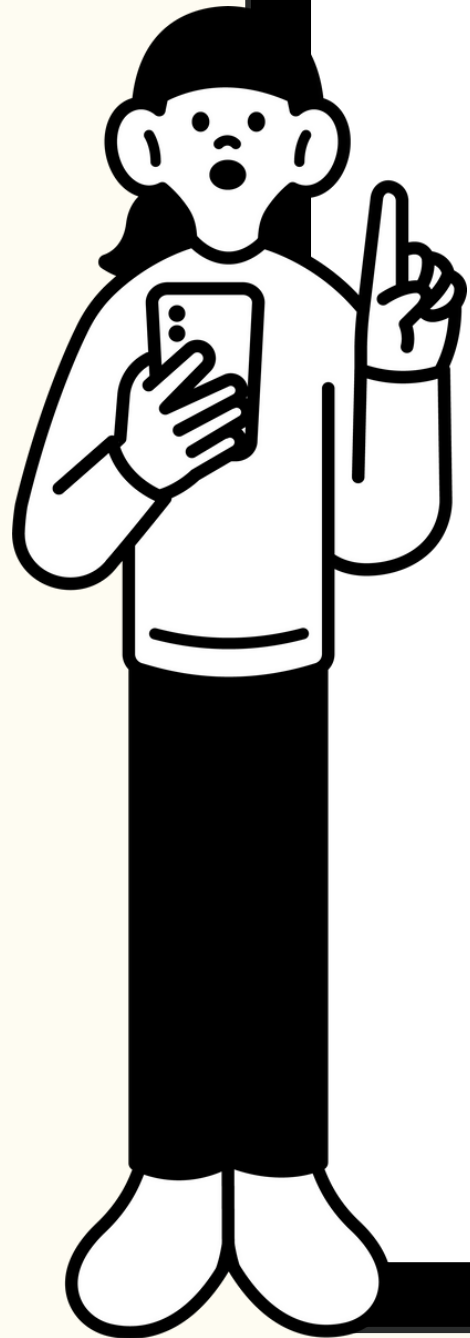


NTT docomo Solutions

セキュリティ教育通信

2026年5月号

NTTドコモソリューションズ株式会社



2026年5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、シンプルに分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

いつもの仕事も外出先だとリスクになる？

2

インターネットの脅威 | Online Threats

知らない間にあなたも加害者に

3

季節・社会動向の注意点 | Seasonal Security

何気ない投稿がリスクになる前に

1. いつもの仕事も外出先だとリスクになる？

そこは本当に、

「仕事をして良い場所」ですか？



1. いつもの仕事も外出先だとリスクになる？

場所が変わると、いつもの事もリスクに変わります。

リスク01

のぞき見される



PC画面、資料、チャット内容、顧客情報などが周囲から見える

リスク02

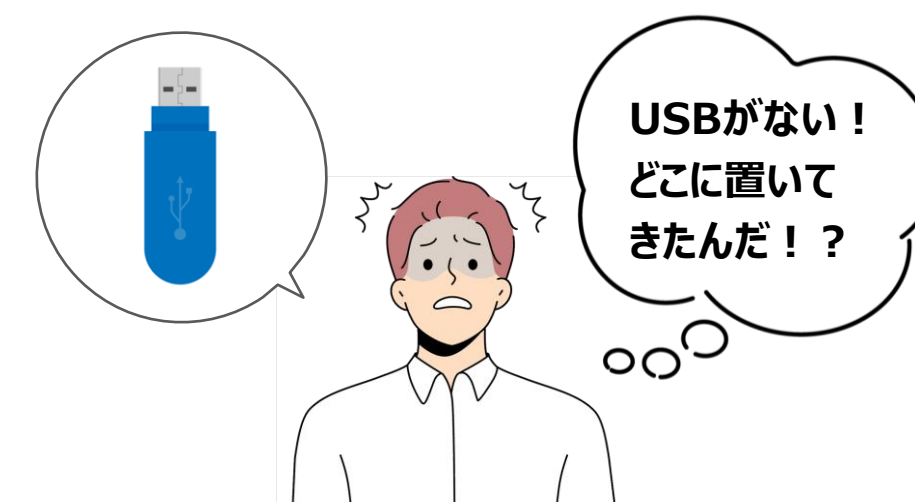
会話を聞かれる



オンライン会議や電話で、社名・案件名・個人情報が漏れる

リスク03

置き忘れ・紛失が起きやすい



PC、スマートフォン、紙資料、USBなどを持ち出すほどリスクが増える

情報漏えいは、特別な攻撃だけで起きるものではありません。

「見られる」「聞かれる」「置き忘れる」だけでも事故になります。

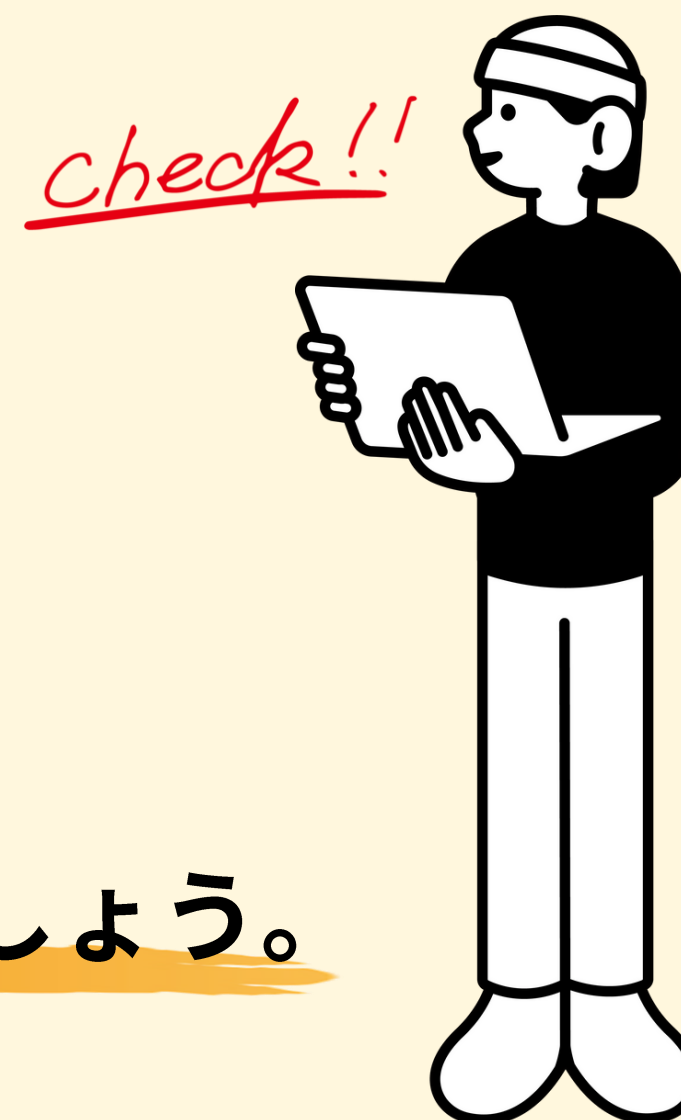
1. いつもの仕事も外出先だとリスクになる？

外出先で仕事をする際に、確認したいこと

- その場所は、会社が作業場所として認めているか
- 周囲から画面や資料を見られないか
- 会話や会議の内容を聞かれる心配はないか
- 端末、資料、記録媒体を紛失していないか

判断に迷ったら、その場で仕事はしない。

“できる場所”ではなく、“してよい場所”かで判断しましょう。



2. 知らない間にあなたも加害者に

有名な予約サイトでホテル予約したのに だまされたー!!



《 騙されるまでの経緯 》

- 1 公式の旅行予約サイトで宿泊を予約
- 2 予約後、ホテル名義の請求メールが届き、案内に従いクレジットカードで支払いを実施
- 3 支払い後、クレジットカード会社から連絡、不正利用の疑いでカードが停止

さて、何がいけなかったのでしょうか？

参考：<https://cybersecurity-jp.com/contents/data-security/1385/>

2. 知らない間にあなたも加害者に

実はこの時、
最初に ホテルが攻撃 されていたんです！

攻撃者の手口とは

01 予約客を装って
ホテルに不正メールを送る



02 ホテルのPCを
マルウェアに感染させる



03 ID・PWを盗み
予約管理システムに侵入



04 顧客情報を元に
連絡経路を悪用し
予約客に偽請求書を送付



予約客は疑うことなく
支払いをしてしまう



攻撃者は **本物の情報** を使うので、**誰でも** 騙されてしまいます。

2. 知らない間にあなたも加害者に

この事例（ホテル側）は、決して他人事ではありません。

- ✓ 業務でも、自分や自社が「侵害される側」になった場合、気づかないうちに **取引先・お客様への被害の入口** になり得ます。
- ✓ “自分の被害”で終わらず、結果的に **取引先やお客様の被害** に繋がってしまうかもしれません。



大切なことは、

「自分が攻撃の入口になり得る」

という視点を持つことです。



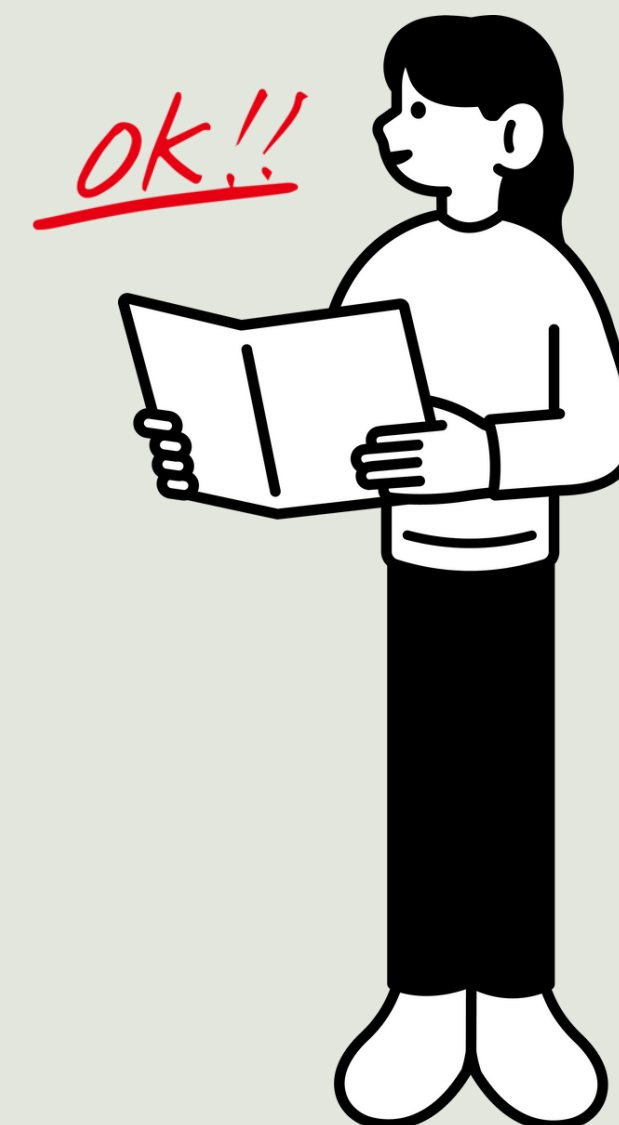
2. 知らない間にもあなたも加害者に

今日からできるチェックリスト

- 業務メールや案内を鵜呑みにせず、必ず一呼吸おく
- 迷ったら“自分で判断しない”と決めておく
- 会社アカウント情報は“狙われる前提”で扱う
- 自分の行動が、取引先・お客様に影響する可能性を意識する

見抜けなかったことが問題なのではありません。

すぐに報告・相談することが大切です。



3. 何気ない投稿がリスクになる前に



攻撃者は些細な情報を見逃しません。

あなたは大丈夫ですか？

3. 何気ない投稿がリスクになる前に

SNSは友達だけが見ているとは限りません

投稿は「点」でも、積み重なると「線」になります

何気ない投稿、
全部繋げて
見られているかも？



不在



「いま旅行中」の投稿＝留守のヒント

リアルタイム投稿は“自宅が空いている”サインになり得ます

場所



過去の投稿・写真の背景＝住所や生活圏のヒント

場所がわかる投稿が続くと、行動範囲や拠点が推測されることがあります

業務との
接点



空き巣などの被害に遭うと「仕事」に波及することも

PCやスマホなど“アカウントにつながる端末”が盗まれると、
個人の被害だけでなく業務にも影響が出る可能性があります

私生活での何気ない行動が、結果的に「業務のリスク」にならないよう、

投稿のタイミングと中身を少し意識しましょう。

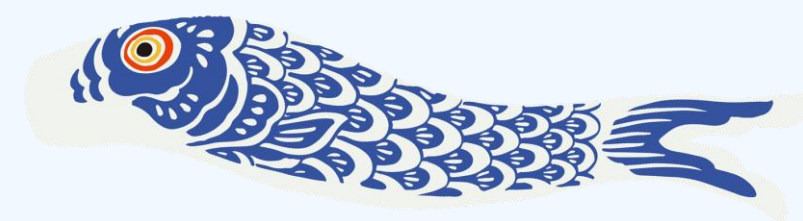
3. 何気ない投稿がリスクになる前に



今日からできる！

投稿前30秒これだけチェックリスト

- 時間をずらして、リアルタイムの投稿は避ける
- 誰が見ているか分からないので、公開範囲を最小限にする
- 撮影・投稿時は位置情報（GPS）をOFFにする
- 個人情報が分かる写り込みがないか確認する



一番大事なことは、

誰が見ても問題ない内容にすること

投稿するタイミングと中身を調整するだけでリスクは下げられます。