

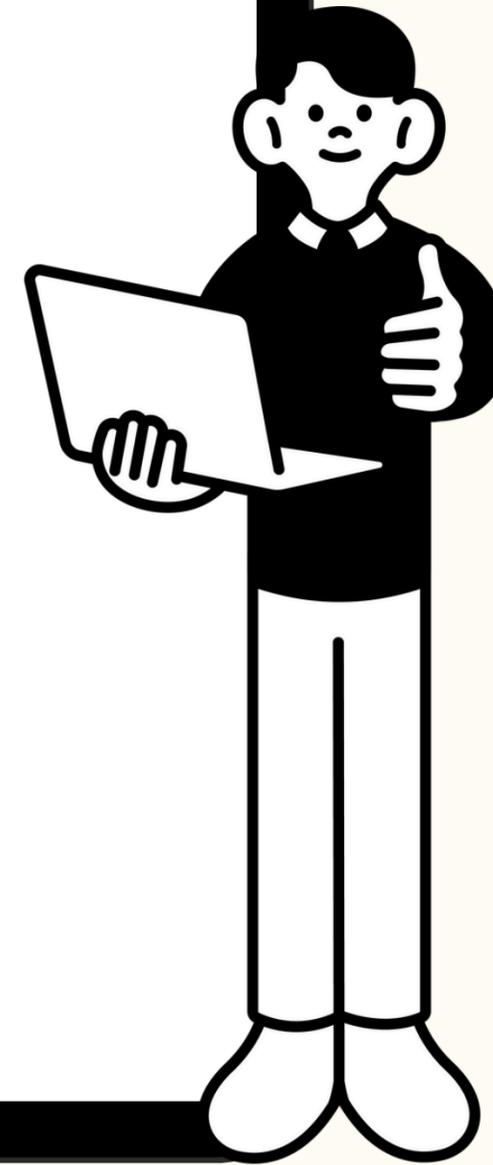
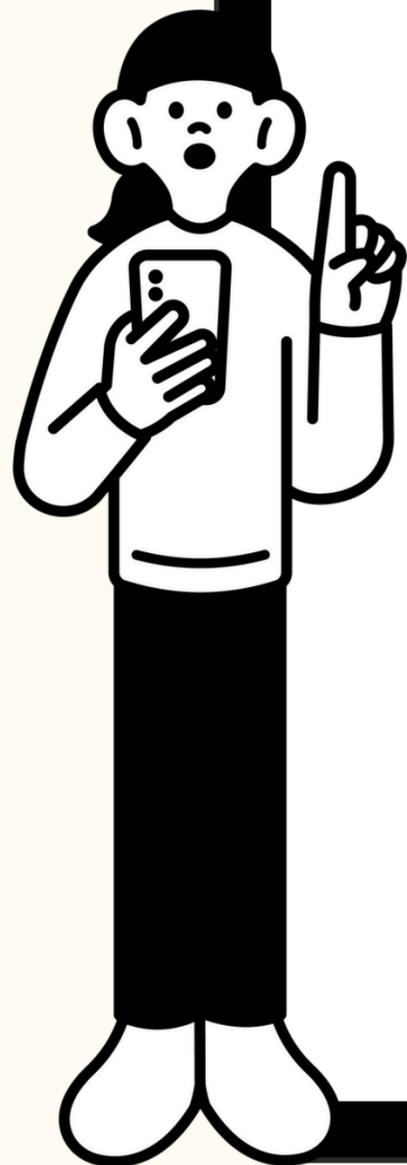


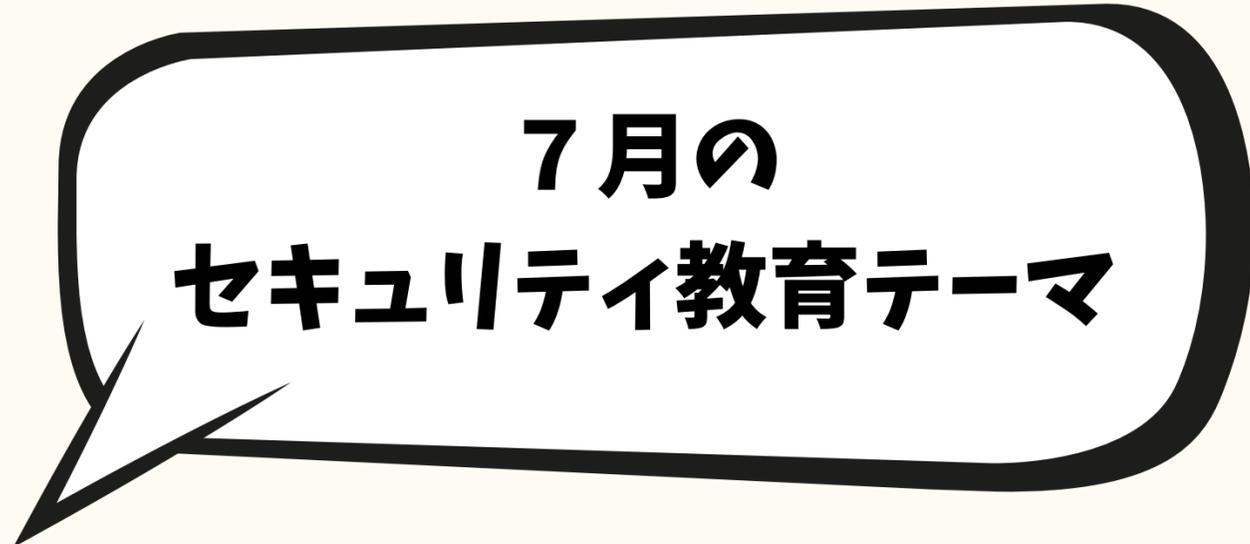
NTT docomo Solutions

セキュリティ教育通信

2025年7月号

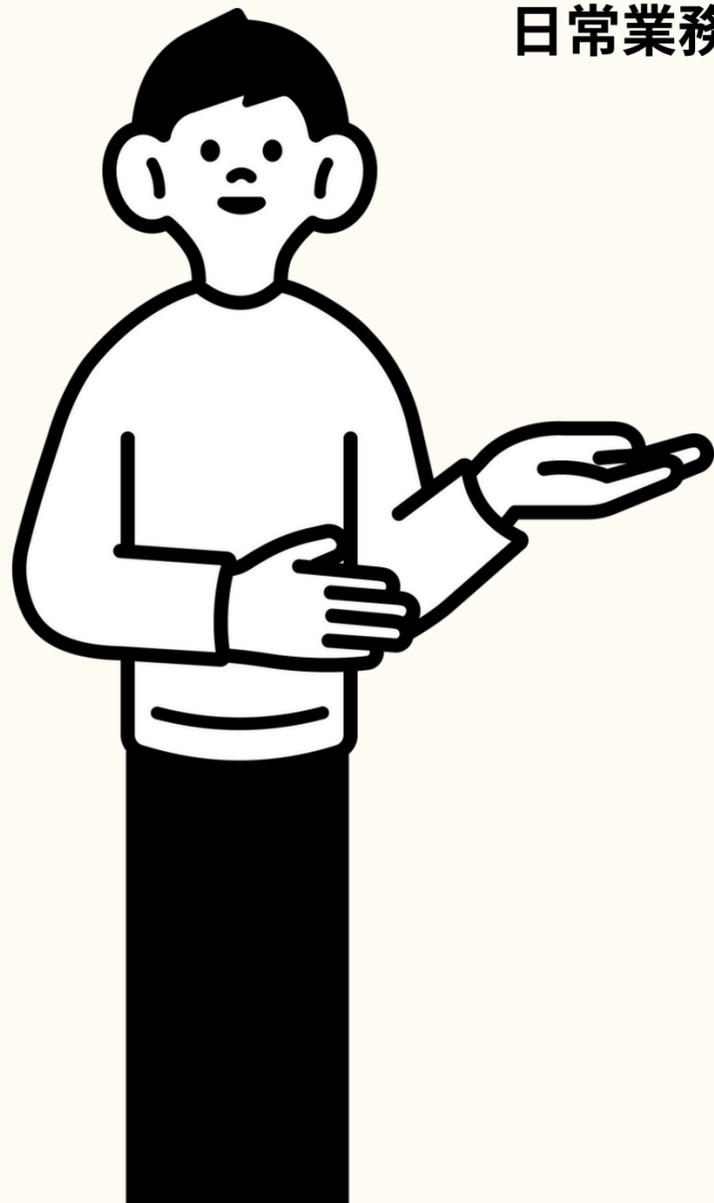
NTTドコモソリューションズ株式会社





7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

スクリーンロック・離席時の端末管理

2

インターネットの脅威 | Online Threats

サポート詐欺を目的とした悪質なサイトに注意

3

季節・社会動向の注意点 | Seasonal Security

夏季休暇におけるセキュリティ対策

1. スクリーンロック・離席時の端末管理

ちょっと席を離れる...その“たった一瞬”が、、、

実は^約**45%**^{*}の情報漏えいが、
“人のうっかり”から始まります！



※IBM Security 2024調査

1. スクリーンロック・離席時の端末管理

席を離れる＝情報漏えいのリスク

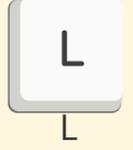
ロック 1 秒、情報漏えい防止



【リスク】

- ✓ のぞき見による情報漏えい
- ✓ なりすまし操作・社内外への不正送信
- ✓ データの無断コピー・持ち出し

【対策】

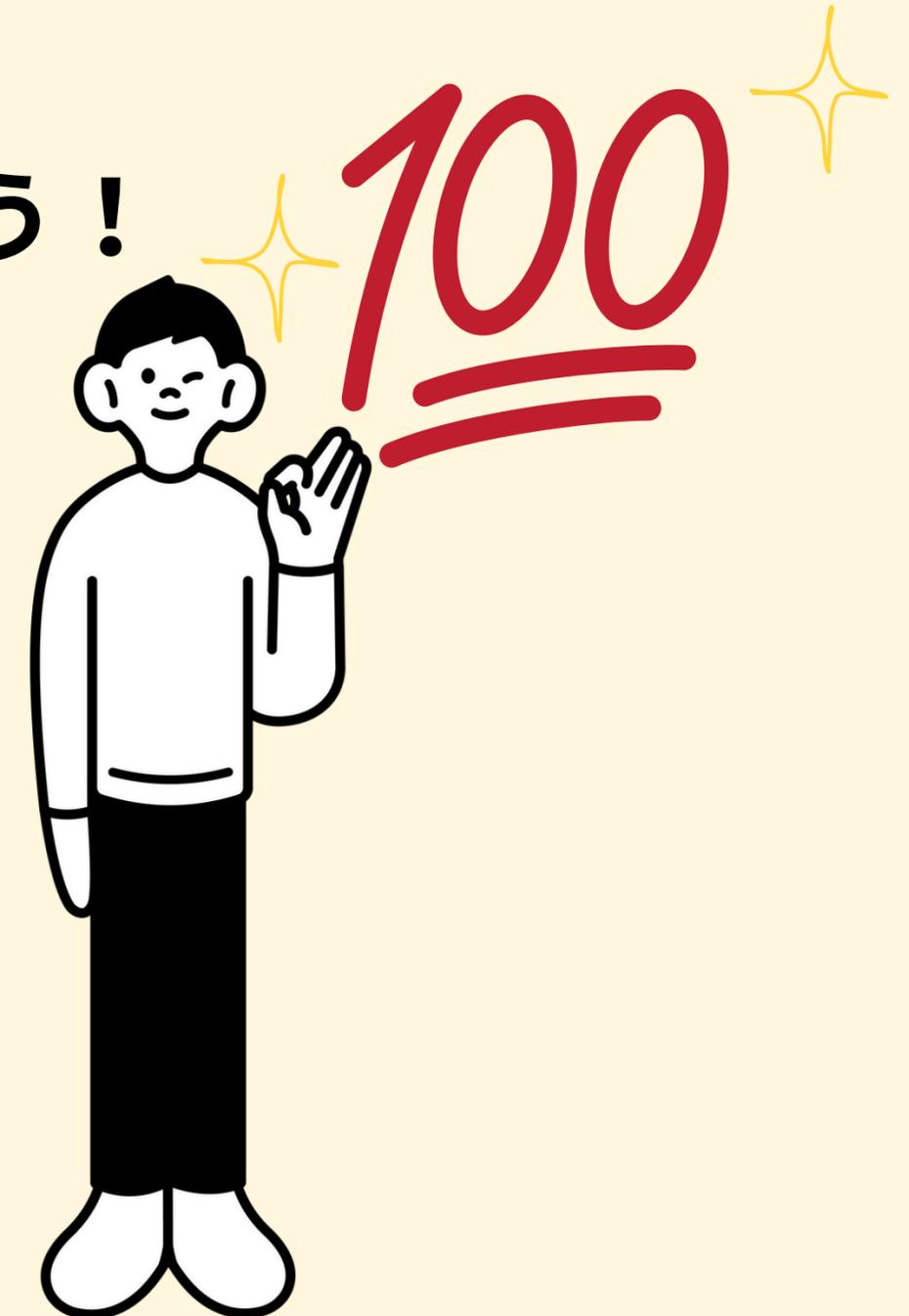
- ▶ 席を離れる時は【 + 】でロック
- ▶ 自動ロック設定も確認（10分以内推奨）
- ▶ 長時間離席時は電源オフ or スリープを

1. スクリーンロック・離席時の端末管理

できてる？

あなたの離席ルールをチェックしよう！

- 席を離れる前に、毎回ロックしている
- 自動ロックが10分以内に設定されている
- チャットや顧客画面を開いたままにしていない
- 誰かが通る席では特に注意している
- ロックすることが“当たり前”になっている



2. サポート詐欺を目的とした悪質なサイトに注意

「ウイルス感染しました！」



...待って！

それ、**サポート詐欺** かもしれません。

2. サポート詐欺を目的とした悪質なサイトに注意

突然、画面がフリーズして「ウイルスに感染しました」「今すぐ電話を」などと表示されます。しかもMicrosoftなどを装い警告音やポップアップで、どんどん不安を煽られます。



画像出典：Microsoft公式ブランド資産ガイドライン ([リンク](#))

⚠ 特徴 ①：画面が勝手にロックされ、警告音が鳴る
ブラウザの偽操作。OSやウイルス対策ソフトの警告ではない。

⚠ 特徴 ②：「すぐに電話を！」と電話番号を表示
正規企業は電話でのサポート誘導を突然表示しない。

⚠ 特徴 ③：「遠隔サポートで直します」と言われる
アクセスさせて金銭を要求するのが目的！



様々な表現で不安を煽るが、焦らず冷静に対処することが大切です。

1. 電話をかける等の案内には従わず、**すぐにブラウザを閉じる**
2. 念のため、アンチウイルスソフトでフルスキャン実行
3. 適切な**担当者へ必ず報告**する

2. サポート詐欺を目的とした悪質なサイトに注意

あなたならどうする？ サポート詐欺セルフチェック！

<質問>

- ①本物のウイルス警告は、電話番号と一緒に表示される？
- ②ブラウザを閉じられないのはPCが壊れたから？
- ③「遠隔操作します」と言われたら操作させてよい？
- ④パニックにならず、まずは一度落ち着くことが大切？

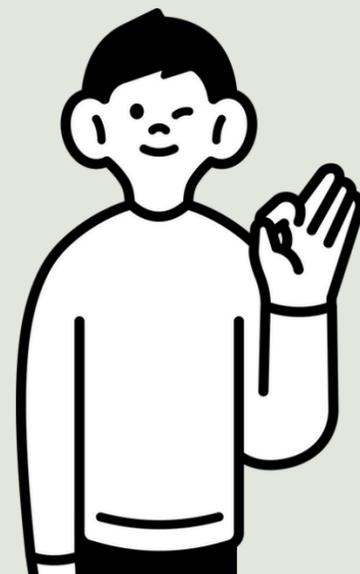
<答え>

×

×

×

○

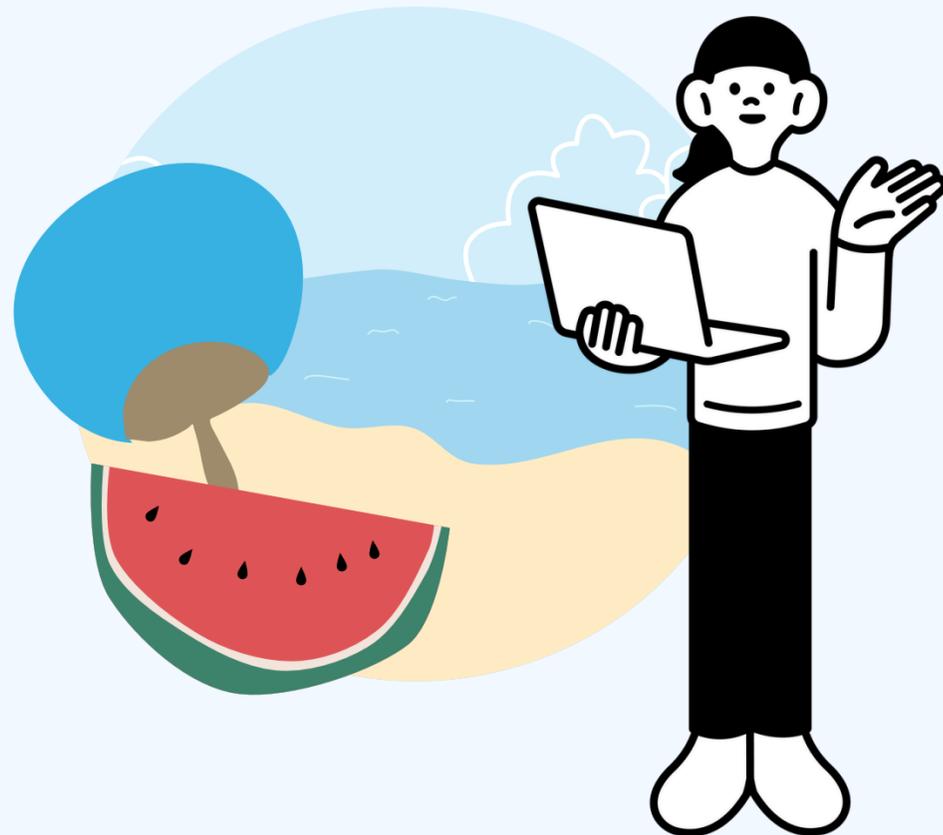


焦りに乗るのが詐欺の手口。
落ち着くことが最大の防御策です。

3. 夏季休暇におけるセキュリティ対策

攻撃は“休暇中”に集中する！

長期休暇中（7～8月）のサイバー攻撃は**最大40%***増加



長期休暇中は、業務が止まり、判断する人も現場にいない状態。

機器は放置され、連絡はつきにくく、
休み明けは、たまった対応に追われてしまう——

そんな“**セキュリティのスキ**”を攻撃者はちゃんと知っています。

3. 夏季休暇におけるセキュリティ対策

夏季休暇に入る前に、次のセキュリティ注意事項を確認しておきましょう。

休暇前

緊急連絡先の確認

〇〇部 緊急連絡先



- ✓ 直属の上司の連絡先
 - ✓ 管理職、統括者などの連絡先
- 業務端末紛失や盗難など、不測の事態に備え連絡先を確認しておきましょう。

休暇中

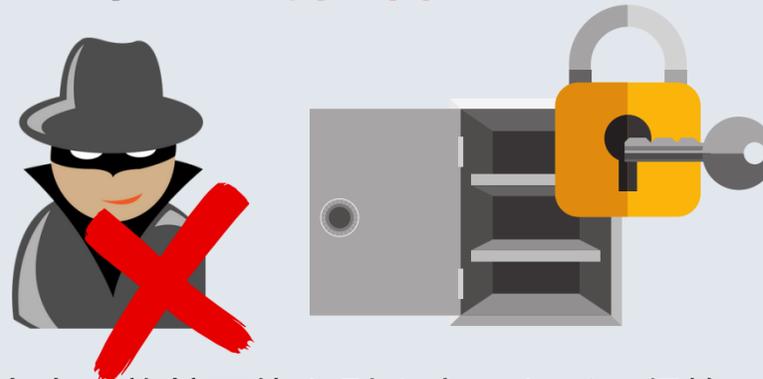
貸与端末の厳重管理

<オフィスにある**使用しないPC**>



- ✓ 会社のキャビネット、デスクの引き出しなどに施錠保管

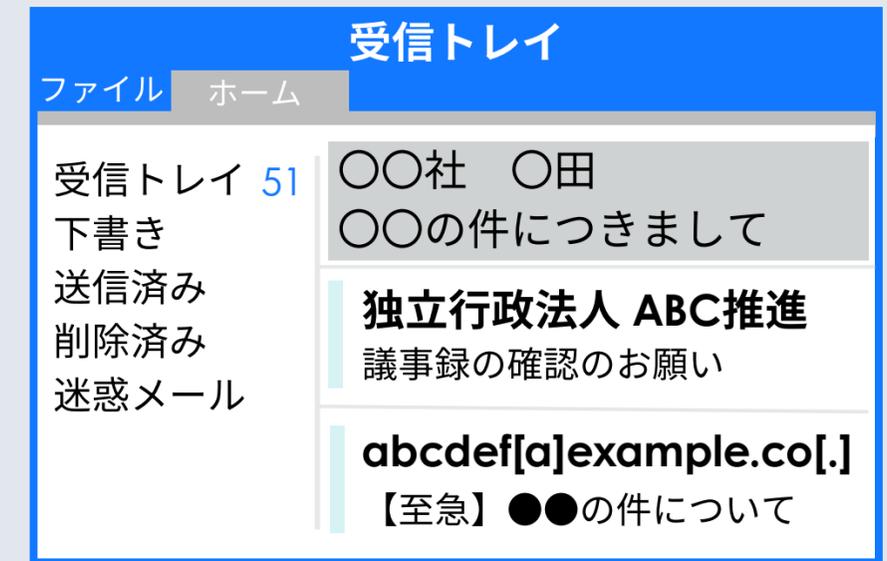
<オフィスから**持ち出しているPC**>



- ✓ 自宅の施錠可能な引き出しなどに保管し、休暇中の盗難対策を徹底

休暇後

不審なメールに注意



- ✓ 慌てて一気に開封しない
- 休暇明けは焦りがち。
怪しい差出人・不自然な日本語は、すぐ開かず、まず慎重に。

3. 夏季休暇におけるセキュリティ対策

夏季休暇のセキュリティ対策、理解できていますか？（確認テスト）

Q1：休暇前に必要な対応として正しいのはどれ？

- A. 使用していないPCはスリープ状態で放置する
- B. 社外共有リンクはそのままで問題ない
- C. 緊急連絡先や端末管理ルールを確認しておく

Q2：持ち出し端末を休暇中に保管する正しい方法は？

- A. 鞆に入れて机の上に置く
- B. 自宅の引き出しや金庫など、鍵がかかる場所に保管する
- C. 常に電源を入れ、メールチェックできる状態にしておく

Q3：休暇明けのメール確認で最も注意すべき行動は？

- A. 急ぎのメールをすぐ開封して処理を始める
- B. 件名と差出人を確認し、不審なものは開かず慎重に対応する
- C. メールはすべて信頼できるので一括開封して問題ない

正しく理解しておくことで、休暇中も“あなたの仕事”と“会社の情報”を守れます。



正解：Q1.C Q2.B Q3.B