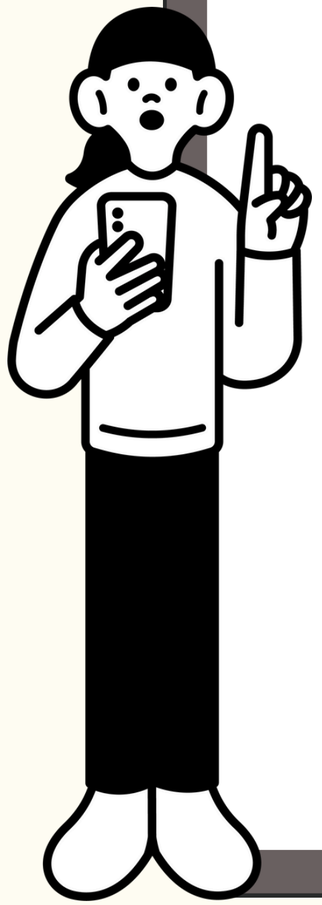
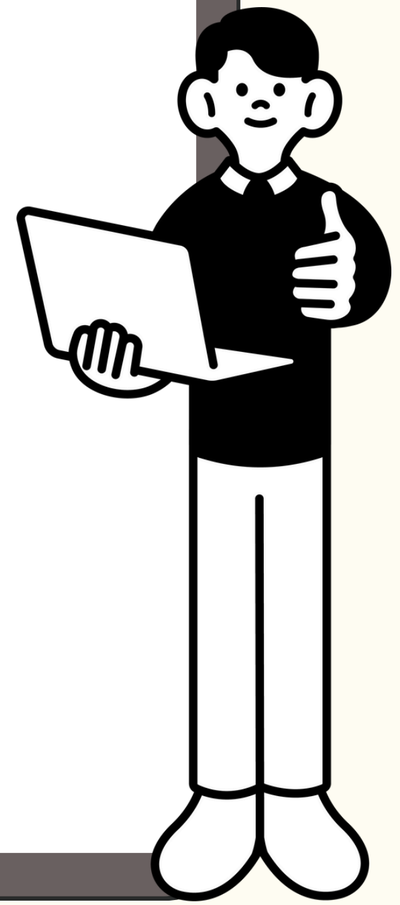


docomo Solutions

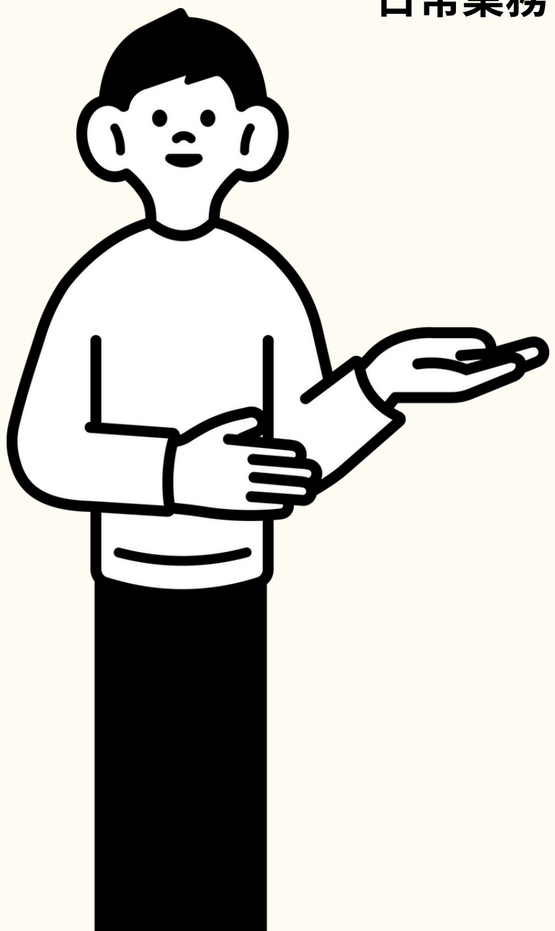
セキュリティ教育通信
2025年 10月号

NTTドコモソリューションズ株式会社



docomo Solutions

10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。

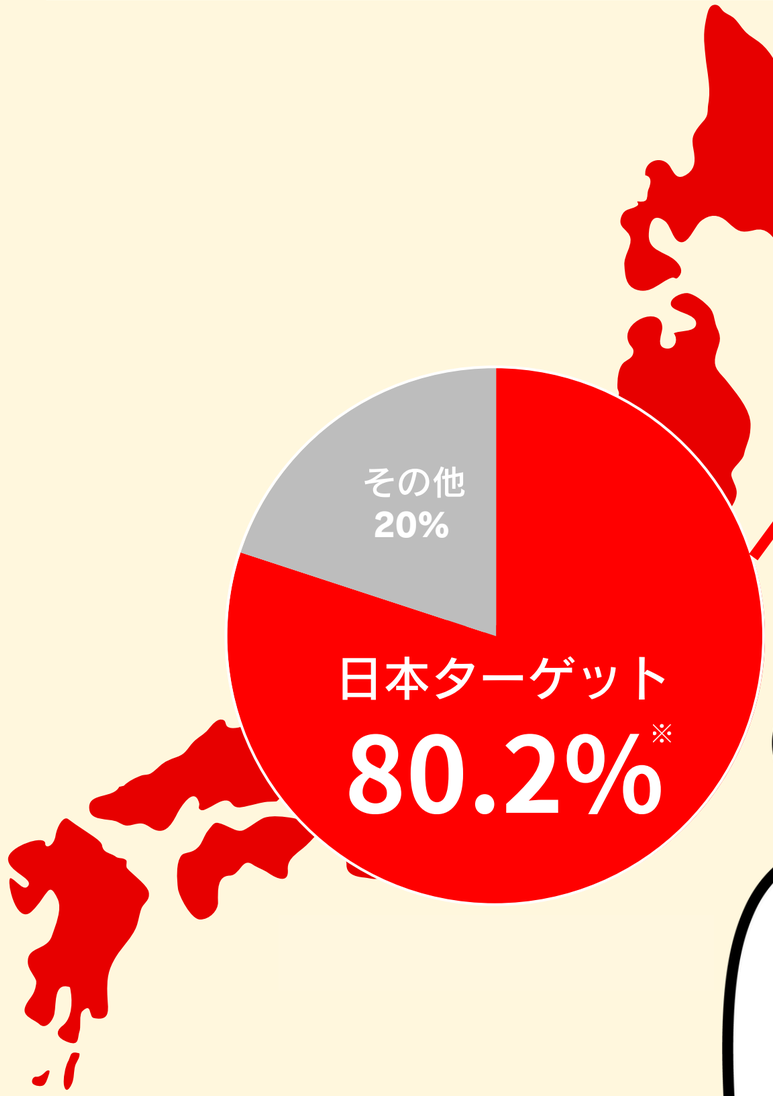
1つ1つのテーマで『なぜ危ないのか』『どう防ぐか』を具体的に紹介していきます。

1
基本対策｜Basic Countermeasures
世界の新しいメール攻撃手口の８割が日本へ

2
インターネットの脅威｜Online Threats
ZIP添付ファイル、開く前にSTOP！

3
季節・社会動向の注意点｜Seasonal Security
人事異動で動く重要情報に注意

１．世界の新しいメール攻撃手口の８割が日本へ



世界で最も狙われているのは日本

その入口の多くは“あなたへのメール”です。

今、日本は世界で
最も多くのメール攻撃を受けています。
そして、そのほとんどがフィッシング詐欺です。

（フィッシング詐欺＝本物そっくりのメールやサイトでだまし、パスワードやカード情報などを盗む手口）

※出典：Proofpoint Threat Intelligence（ブログ「日本が今、最も狙われている？ 急増するDDoS攻撃とメール攻撃の実態」より）

１．世界の新しいメール攻撃手口の８割が日本へ

なぜ日本がこれほど狙われるのか？

01 攻撃の集中

- 2025年2月、世界で確認された **“新しい手口のメール攻撃” の 80.2% が日本を標的。**
- わずか2か月後の4月には **83.6% に増加。**
- **世界で最も多く攻撃を受けている国が日本。**

02 背景にある変化

- **生成AIの進化**で、誰でも自然な日本語の**詐欺メール作成が容易**になった。
- 以前は日本語の不自然さで見抜けたが、今は見抜きにくくなってきた。
- **「自然な日本語＝安全」**という**思い込みが逆にリスク**となる時代。

03 日本が狙われる理由

- **個人情報・決済情報が闇市場で高値取引**される。
- 日本企業が持つ**技術・取引情報は世界的に価値が高い。**
- **詐欺の成功率が比較的高い**日本市場＝攻撃者にとって効率が良い。
  日本の成功被害率 64%（Proofpointによる「成功率」に関する国際比較）

これは、私たち一人ひとりに向けられた攻撃です。

１．世界の新しいメール攻撃手口の８割が日本へ

☑理解度チェック｜身につけた知識をテスト

Q1：2025年2月、世界の新種メール攻撃のうち、日本を標的にした割合は次のうちどれでしょう？

A. 8.2%

B. 80.2%

C. 38.6%

Q2：生成AIにより、日本語の自然な詐欺メールも簡単に作れるようになった。正しい理解はどれ？

A. 自然な日本語なら安全

B. 自然な日本語でも詐欺の可能性がある

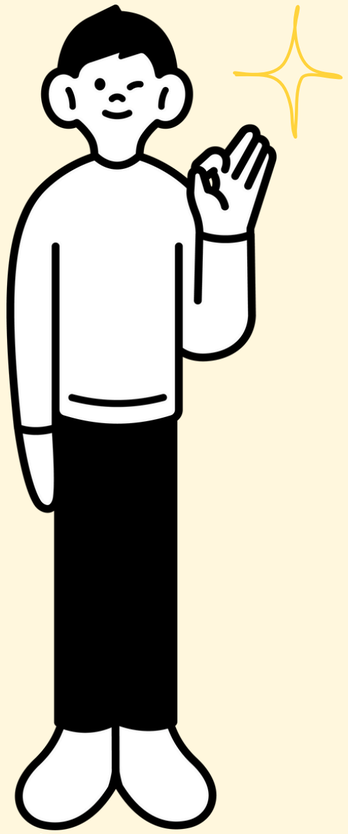
C. 自然な日本語は必ず詐欺

Q3：日本が狙われる理由として正しいものはどれ？

A. 個人情報や決済情報が価値の高い資産だから

B. 日本語は攻撃者にとって難しいから

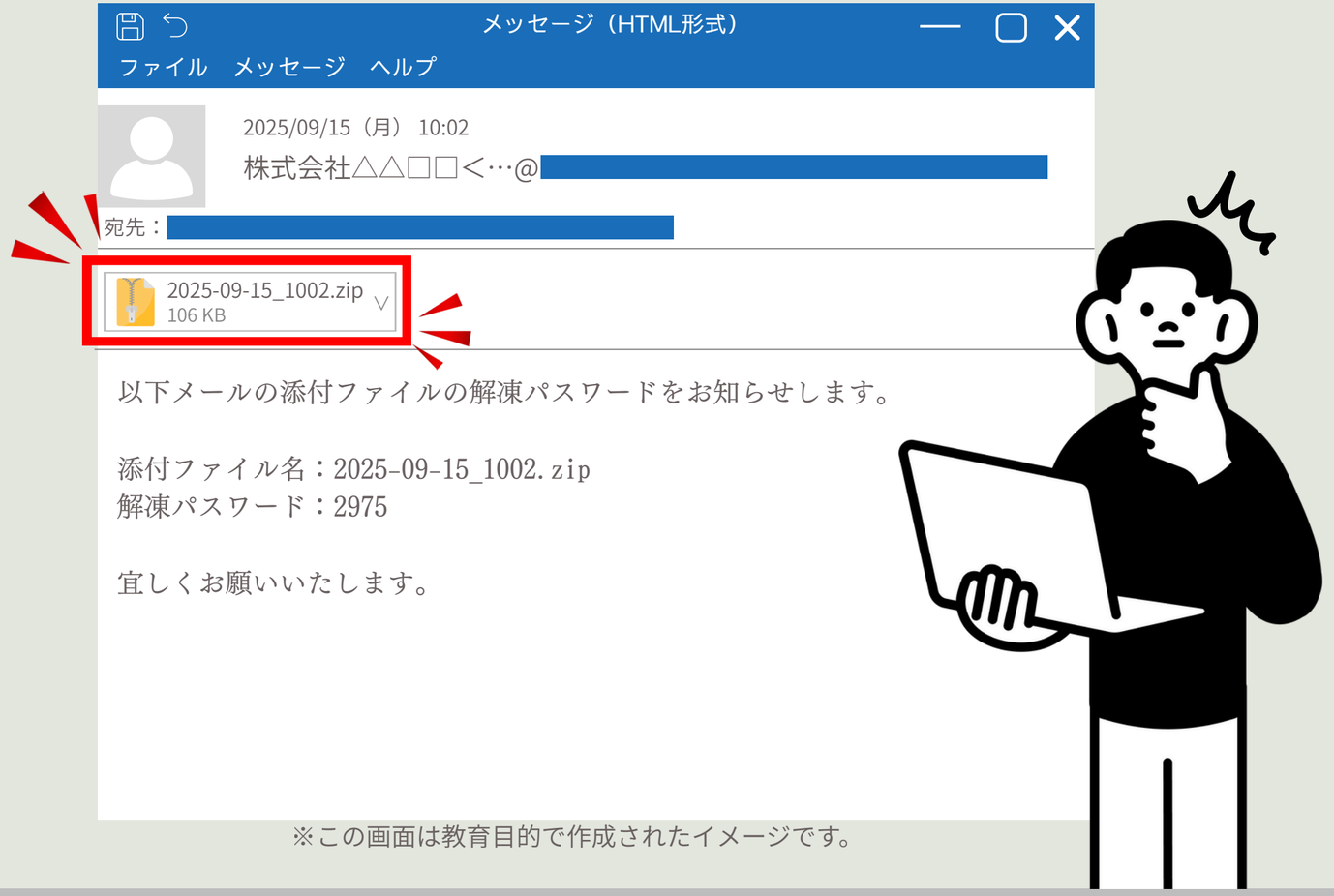
C. 日本はインターネット利用者が少ないから



正解：Q1.B Q2.B Q3.A

２．ZIP添付ファイル、開く前にSTOP！

その添付、安全に見えて危険かも！？



※この画面は教育目的で作成されたイメージです。

２．ZIP添付ファイル、開く前にSTOP！

「なぜZIPファイルは危険なのか？」

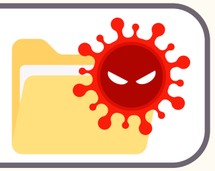
その理由を知って、だまされない力をつけましょう。

危険とされる
3つ の理由

1 ウイルス検知をすり抜ける
パスワード付きZIPはセキュリティソフトが中身を検査できない

2 見た目が“普通”で安心されやすい
社内資料や業務データのやり取りに似ていて疑われにくい

3 解凍した瞬間に感染する
Word/Excelマクロや.exe形式でマルウェアが実行される



添付を開く前に、必ず送信元や内容の妥当性を確認してください

２．ZIP添付ファイル、開く前にSTOP！

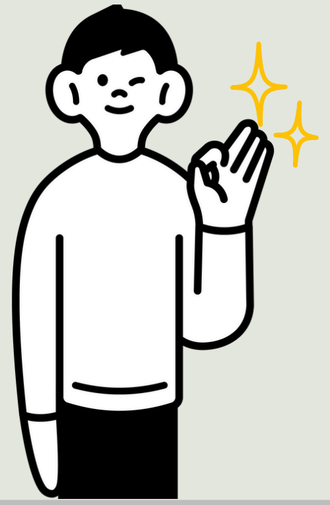
理解度チェック｜だまされない力をテスト

Q1：パスワード付きZIPファイルが危険とされる理由はどれでしょうか？

A. セキュリティソフトが中身を検査できないから
B. 保存できないから
C. 開くと自動的に削除されるから

Q2：見た目が普通に見えて受信者が安心してしまいやすいのは、どんな点からでしょうか？

A. 社内資料や業務データのやり取りに似ているから
B. ZIPはサイズが小さいから
C. メールの件名が短いから



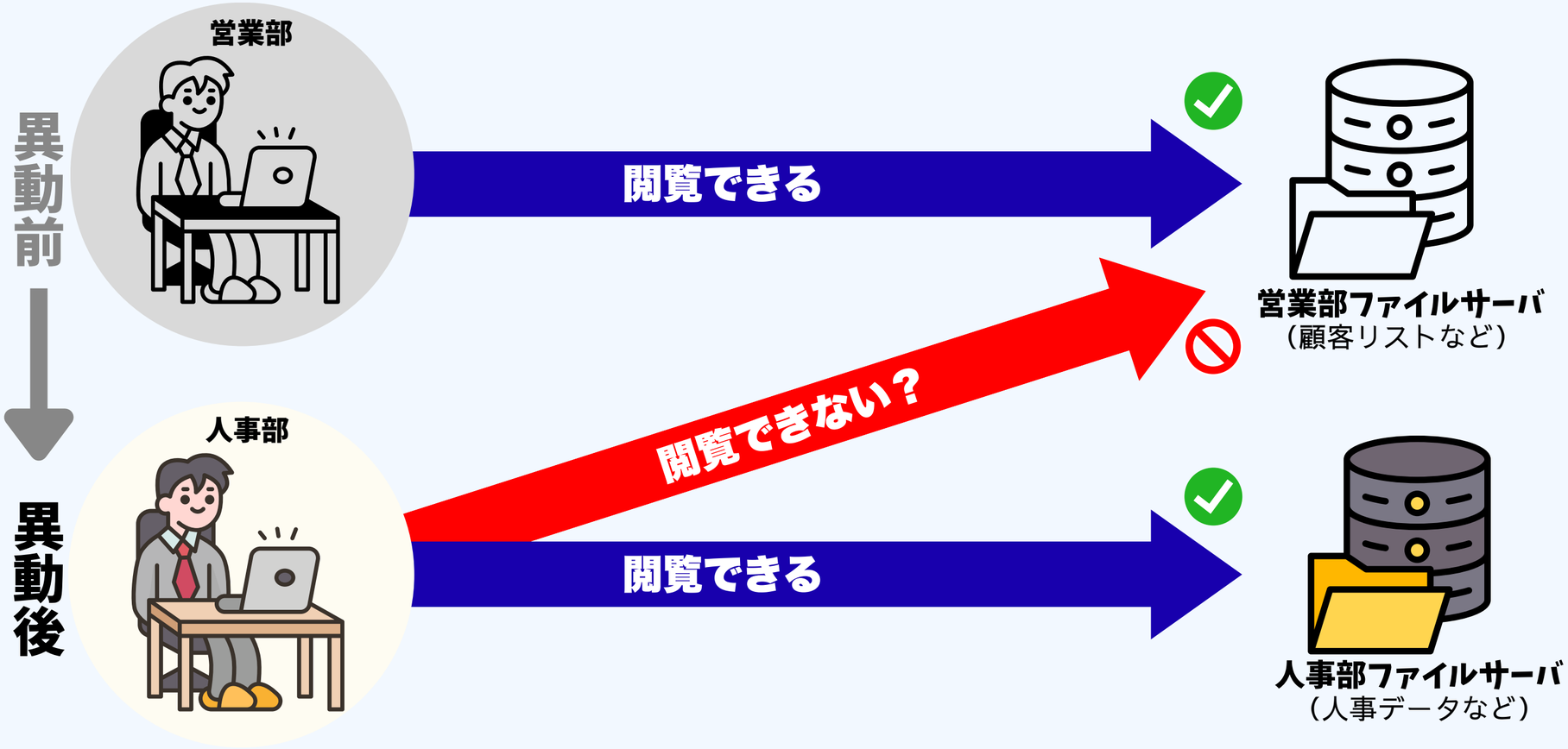
Q3：もし不審なZIP添付メールを受け取った場合、最も安全な行動はどれでしょうか？

A. すぐに解凍して中身を確認する
B. 上司やシステム管理部門に相談し、送信元や内容の正当性を確認する
C. 念のため同僚にも転送して確認してもらう

正解：Q1.A　Q2.A Q3.B

３．人事異動で動く重要情報に注意

人事異動後も見えてしまう情報ありませんか？



３．人事異動で動く重要情報に注意

異動時に守るべき情報の取り扱いルールを確認しましょう。

1

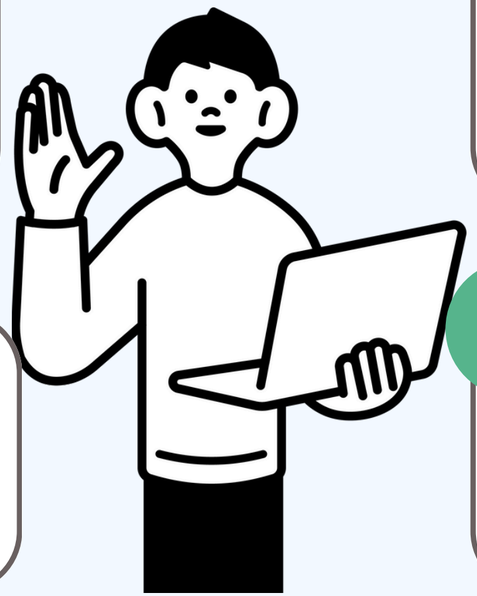
知る必要のない情報は見ない

間違って利用・流出のリスクを防ぐ

2

異動前にデータは整理する

自分の端末やメール、クラウドの不要データを整理



3

不要なデータは持ち出さない

引き継ぎに関係ないファイルやUSBは削除・返却

4

共有は最小限に

必要な相手・範囲だけに情報を渡す

特に異動のときは情報の取り扱いは、要注意です。

３．人事異動で動く重要情報に注意

☑ 異動前後に確認すべき情報管理のポイント

□ 不要になった共有フォルダやデータにはアクセスしない

□ 端末・メール・クラウドデータは会社のルール通りに整理する

□ 机・ロッカーに残された不要データは破棄する

□ 私的なクラウドやUSBには業務データを保存しない