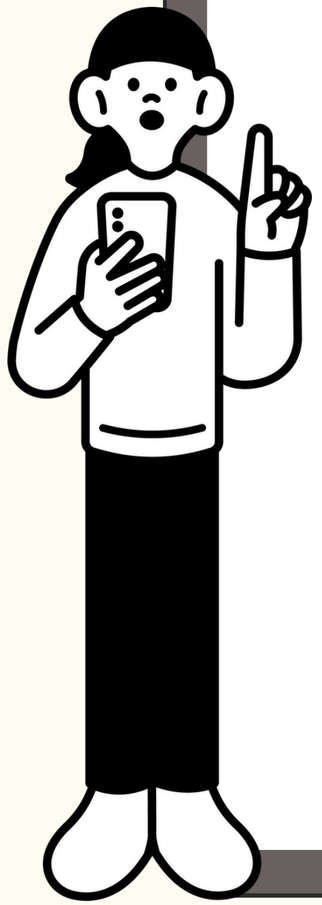
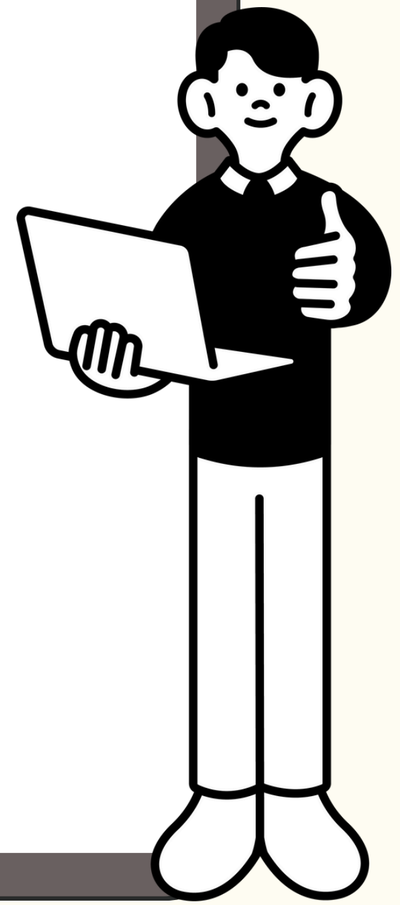


docomo Solutions

セキュリティ教育通信
2025年 9月号

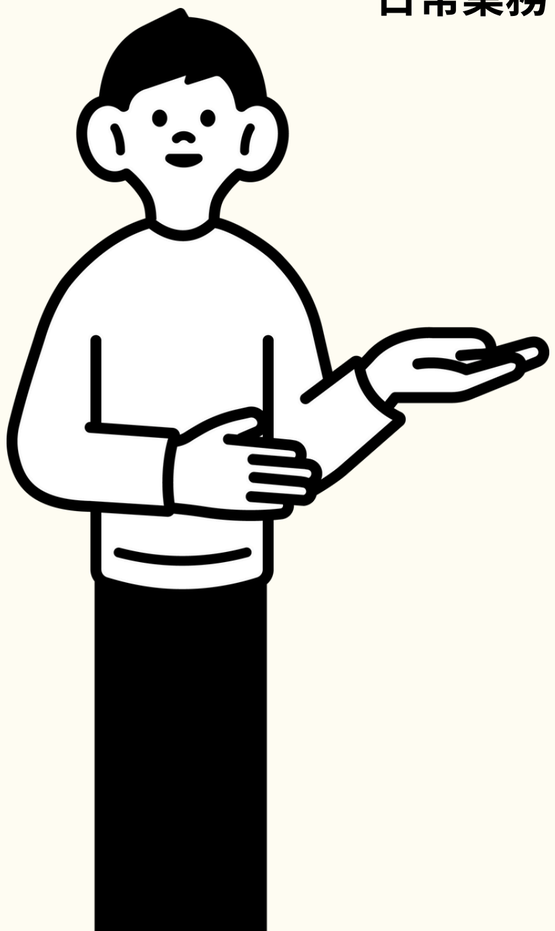
NTTドコモソリューションズ株式会社



docomo Solutions

9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
電話・口頭での情報漏洩リスク

2 インターネットの脅威｜Online Threats
「本物だと思ったら偽物だった…」偽サイトを見抜く3つのポイント

3 季節・社会動向の注意点｜Seasonal Security
災害時の偽連絡に注意しましょう！

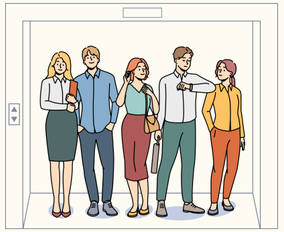
１．電話・口頭での情報漏洩リスク

その会話、誰かに聞かれているかも？

話している内容が、意外と周囲に聞こえているかもしれません。
機密情報やお客様の名前、金額、パスワードなど、
口頭でのやりとりも　**“情報漏洩”の入り口**　になります。

１．電話・口頭での情報漏洩リスク

話す前に ３つ 「場所・周囲・声」のチェックを！



場所に注意！

どこで話している？

通路・カフェ・エレベーターなど、周囲に人がいる場所は要注意！

周囲に注意！

誰が聞いている？

後ろや隣に人がいたら、“聞かれてる前提”で考えよう。

声量に注意！

その声、大きすぎない？

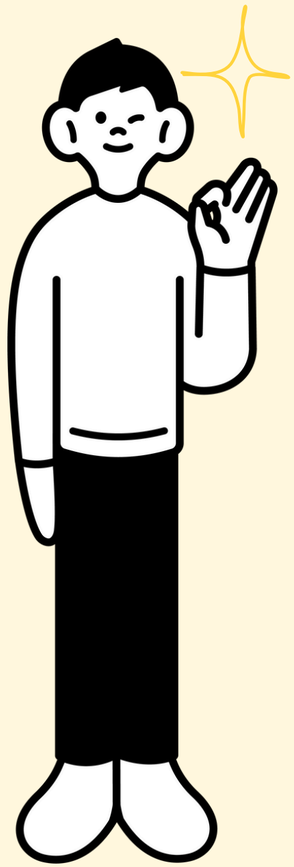
社名・金額・パスワードなどは、声に出す前に再確認！

特に「公共の場」「在宅勤務中」「オフィスのオープンスペース」での会話には注意！

１．電話・口頭での情報漏洩リスク

会話の安全度を今すぐ確認！

行動	YES/NO
社外の人がいる場所は気を付けて機密情報は話さない	□ / □
周囲に第三者がいたので、顧客名や金額を電話で伝えない	□ / □
会議室やカフェなどで声量に気をつけている	□ / □
在宅勤務中、家族であっても聞かれないよう気をつけている	□ / □



２．「本物だと思ったら偽物だった…」偽サイトを見抜く3つのポイント

どちらが本物？　どちらが偽物？

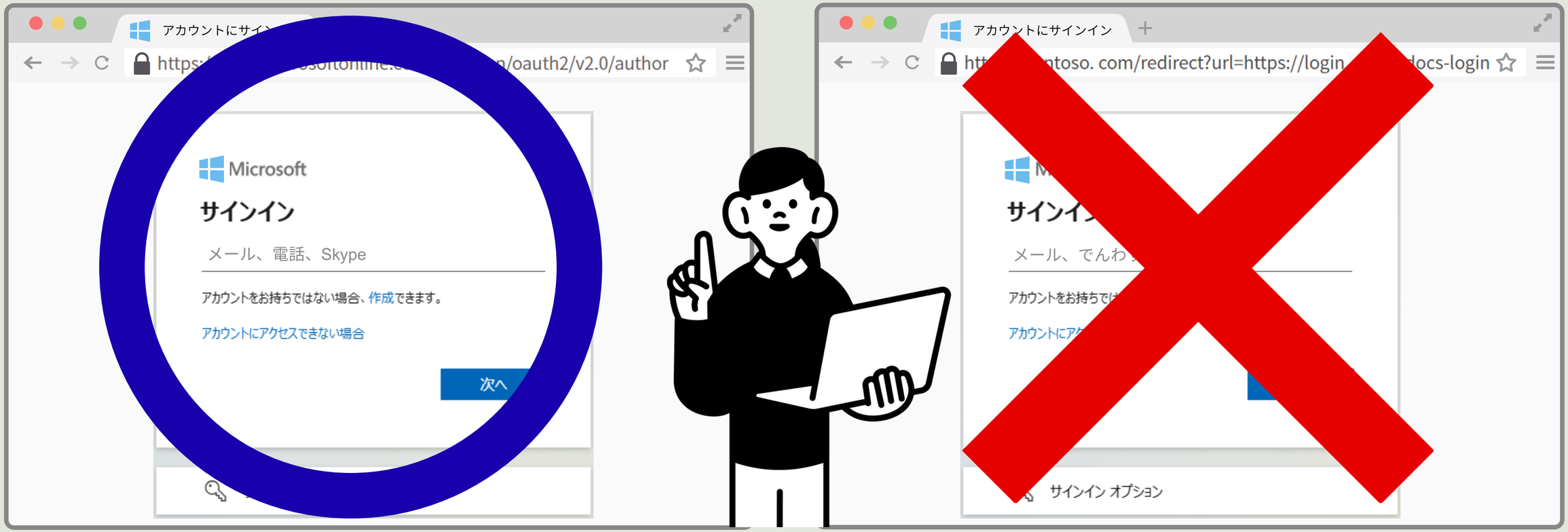
※この画面は教育目的で作成されたイメージであり、Microsoft社とは関係ありません。実際のログイン画面とは異なる場合があります。

２．「本物だと思ったら偽物だった…」偽サイトを見抜く3つのポイント

正解は、

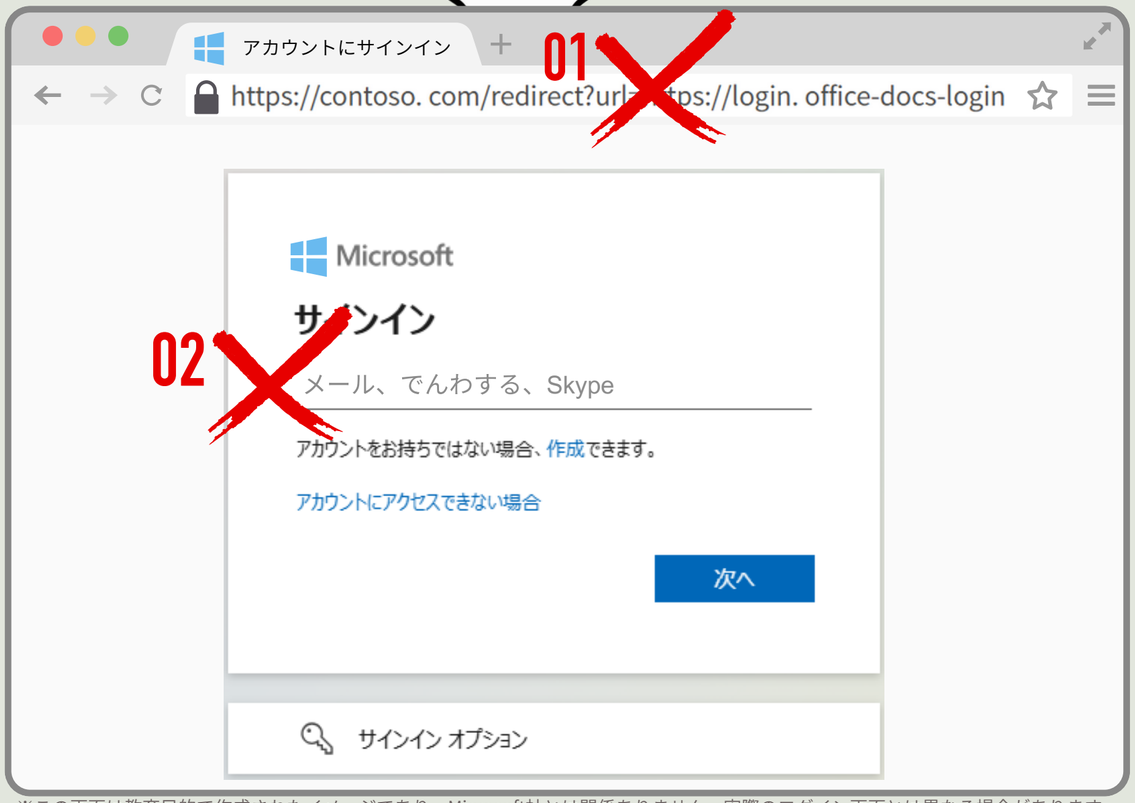
本物

偽物



※この画面は教育目的で作成されたイメージであり、Microsoft社とは関係ありません。実際のログイン画面とは異なる場合があります。

２．「本物だと思ったら偽物だった…」偽サイトを見抜く3つのポイント



※この画面は教育目的で作成されたイメージであり、Microsoft社とは関係ありません。実際のログイン画面とは異なる場合があります。

では、どうやって見抜く？

3つのポイントを解説します。

01 URLのドメインを確認

- 本物：login. microsoftonline.com
- 偽物：見慣れないドメイン（例：contoso.comなど）や、
  似た文字の置き換えに注意（大文字の「I（アイ）」と小文字の「l（エル）」等）
- 「https」や鍵マークだけでは安全とは限らない

02 不自然な日本語に注意

- 本物：自然な表記（例：メール、電話、Skype）
- 偽物：違和感のある言葉（例：メール、**でんわする**、Skype）
- フォントや文字間隔が微妙に違う場合もある

03 送られてきた経路を疑う

- 突然届いたメールやチャットのリンクからアクセスしない
- 必ず公式サイトやブックマークからアクセス
- 不審に感じたら情報システム部門や管理者に確認

２．「本物だと思ったら偽物だった…」偽サイトを見抜く3つのポイント

あなたの偽サイト見抜き力をチェック！

- □ URLのドメインを必ず確認している
- □ 不自然な日本語やスペルに気づける
- □ メールやチャットのリンクは即クリックしない
- □ 必ず公式サイトやブックマークからアクセスしている

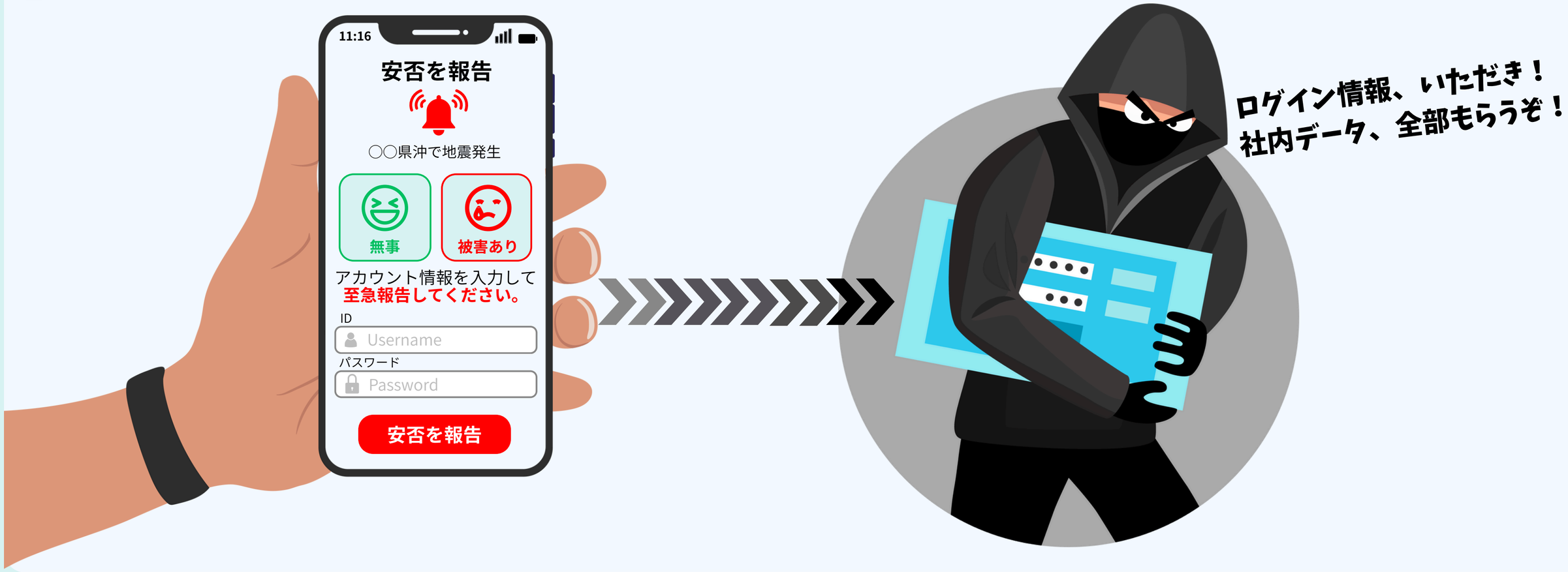
３つ以上チェックがつけば**「合格」**です！
２つ以下なら**「再確認が必要」**ですので前のスライドに戻って確認してくださいね。

季節・社会動向の注意点｜Seasonal Security

３．災害時の偽連絡に注意しましょう！

急増中！

災害の混乱に便乗した“偽安否確認”



docomo Solutions

季節・社会動向の注意点｜Seasonal Security

３．災害時の偽連絡に注意しましょう！

実際にあった「偽 安否確認フォーム」被害

■事例

- 2023年、国内企業で**地震発生直後に「安否確認フォーム」のメールが社員に一斉送信**された。
- 社員が偽画面に**社内アカウントとパスワードを入力**し、情報が盗まれて**社内システムへ不正アクセス**された。

攻撃者は、「災害時の混乱」と「急いで報告しなければ」という心理を悪用してきます。

■対策・注意点

- ☑ メール等のURLをすぐクリックせず、正規のブックマークなどからアクセスする
- ☑ 安否確認の送信元アドレスやドメインを必ず確認する（例： @company.co.jp）
- ☑ 「至急対応」「重要度（高）」と言われても、安易に信じず一呼吸置いて対応する

災害時こそ「冷静な確認」が会社と自分を守りますので、まず落ち着いて！

３．災害時の偽連絡に注意しましょう！

あなたは災害時でも冷静に対応できますか？
チェックしてみましょう！

行動	YES/NO
・災害時は緊急だけど、メールに届いたURLを確認してから報告をする。	□/□
・安否確認フォームが届いたら、送信元アドレスやドメインを必ず確認する。	□/□
・少しでも不審なら、IT部門や上司に相談する。	□/□