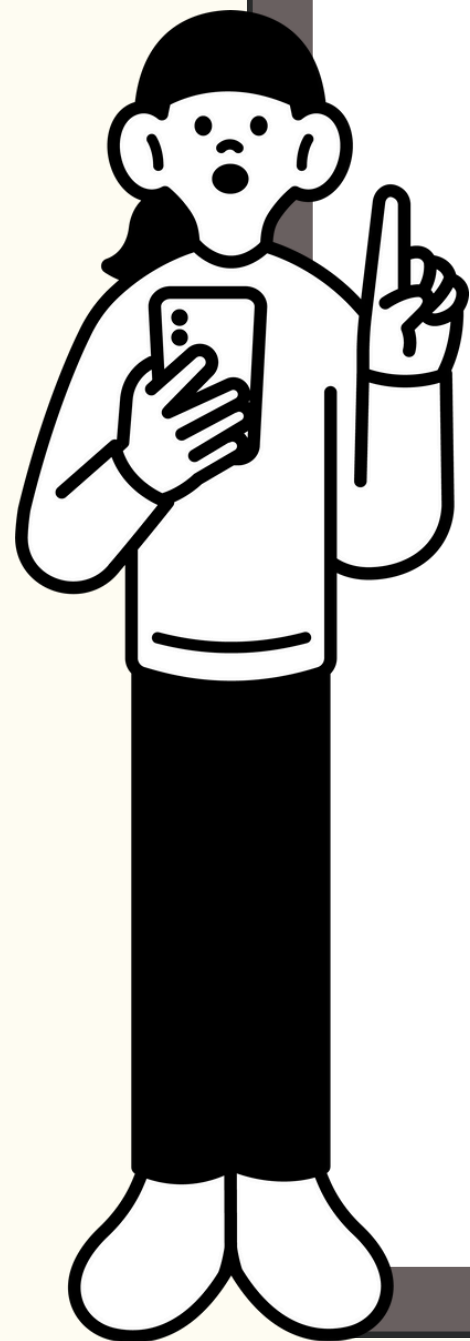




セキュリティ教育通信 2026年 2月号

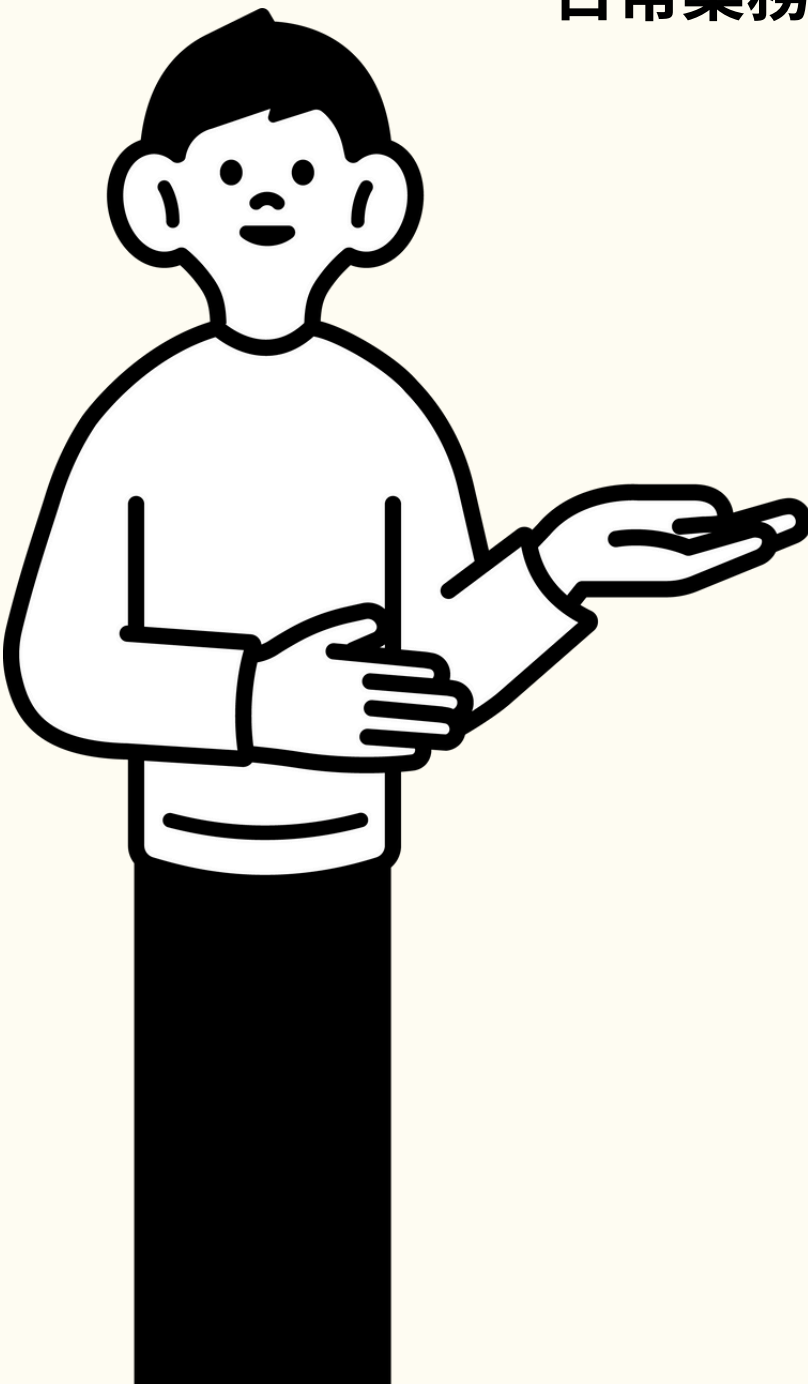
NTTドコモソリューションズ株式会社



2026年2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

なぜ、攻撃者は「なりすまし」を手口に使うのか？

2

インターネットの脅威 | Online Threats

社長名を使った「なりすまし」に注意

3

季節・社会動向の注意点 | Seasonal Security

選挙後に増える「便乗した連絡」に注意

1. なぜ、攻撃者は「なりすまし」を手口に使うのか？

知っている人からの連絡に、

あなたはどのくらい警戒していますか？



1. なぜ、攻撃者は「なりすまし」を手口に使うのか？

人は「知っている人」からの連絡だと、無意識に警戒心を解いてしまいます

これらは全て、人が「警戒心を解く瞬間」を狙った手口です

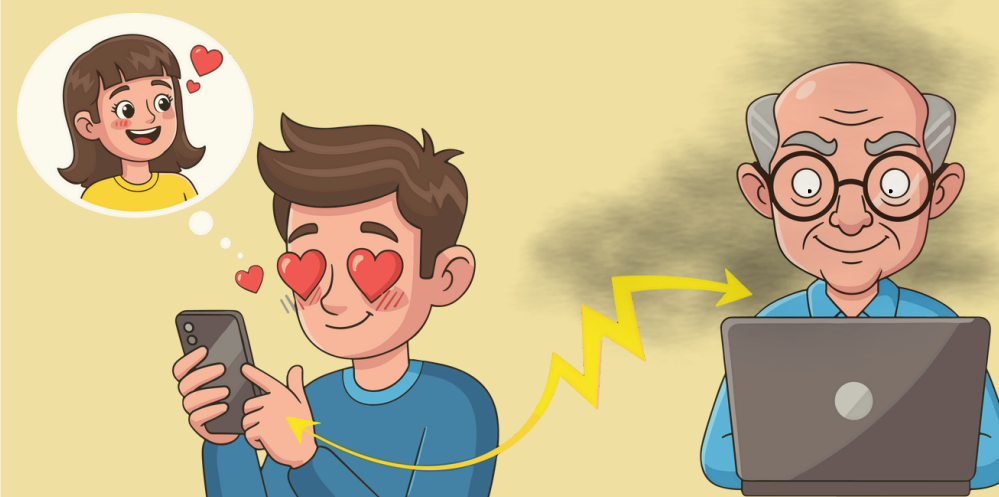
オレオレ詐欺

家族や親族を名乗り、
「今すぐ助けてほしい」と不安をあおることで、
冷静な確認をさせずにお金だまし取る詐欺



なりすまし型フィッシング詐欺

知人のSNSを乗っ取った後にDMで
「インフルエンサー始めたので、応援してほしい」
と連絡が来て対応すると、自分のSNSも乗っ取られる



ロマンス投資詐欺

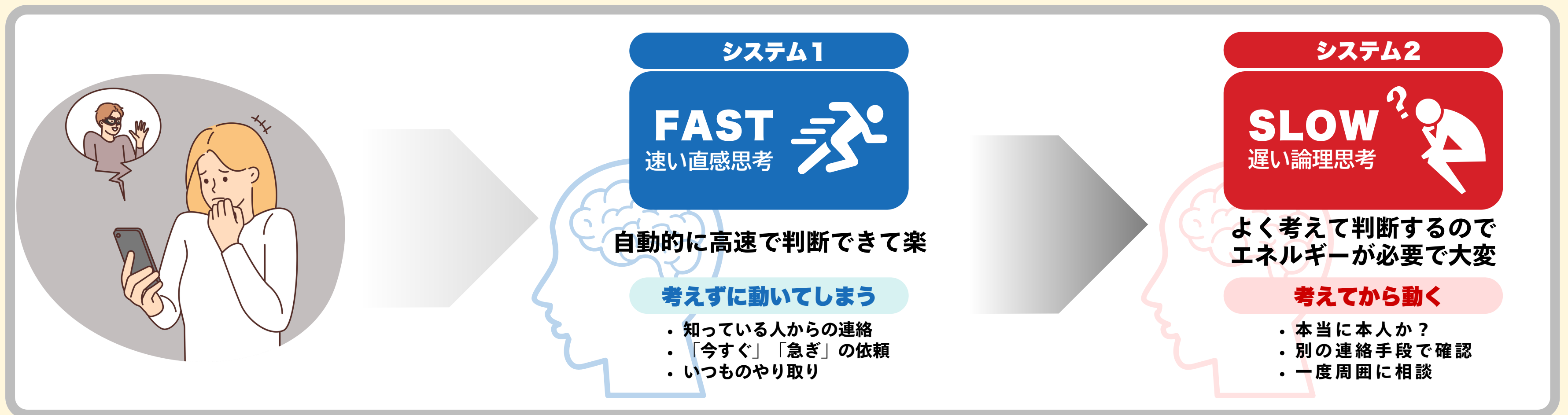
マッチングアプリなどで信頼関係を築いた後、
投資話を持ちかけてお金をだまし取る詐欺



1. なぜ、攻撃者は「なりすまし」を手口に使うのか？

人の脳は、エネルギーを使う判断をなるべく避けるようにできています。

攻撃者は、深く考えさせないように「FAST(直感思考)」を狙っています。



私たちの脳は、楽に判断できる FAST(システム1) を使いがちです。

だからこそ、なりすましは成功しやすいのです。

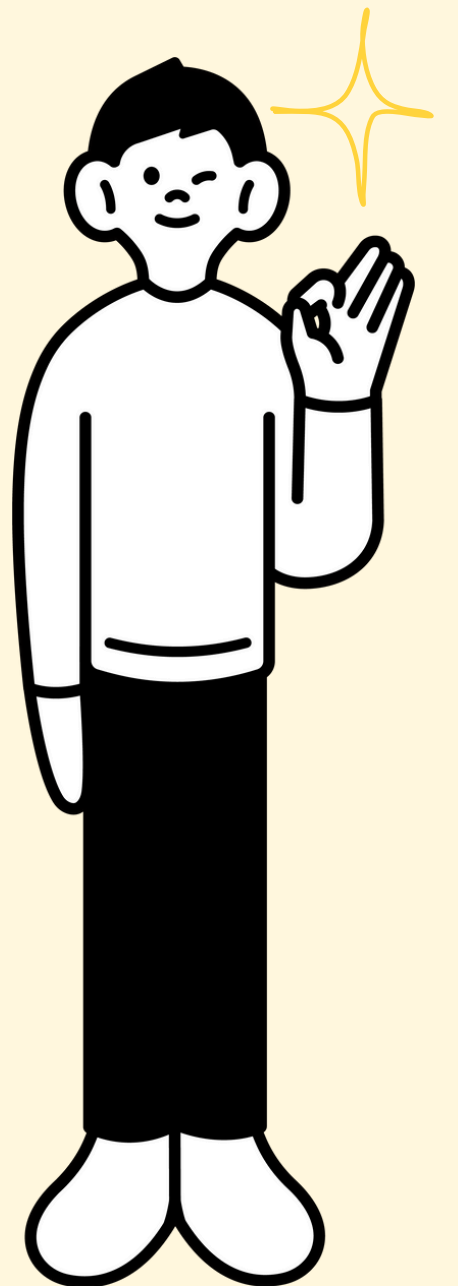
1. なぜ、攻撃者は「なりすまし」を手口に使うのか？

慣れた連絡ほど、立ち止まって確認を。

✓ 理解度チェック

- ☐ 人は「知っている人からの連絡」だと、警戒心が下がりやすい
- ☐ 急ぎ・いつもの依頼は、考える前に判断してしまいやすい
- ☐ なりすましは、人の「速い思考(FAST)」を狙った攻撃である

「いつも通り」と感じた瞬間こそ、
一度立ち止まることがセキュリティです。

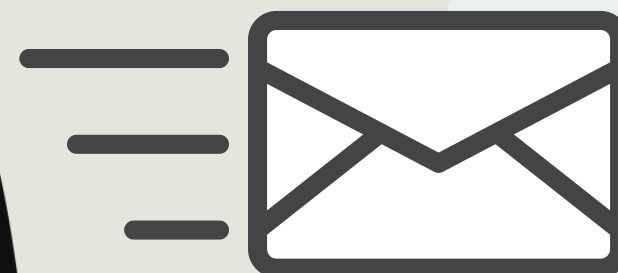


2. 社長名を使った「なりすまし」に注意

社長から業務指示メールが届きました
あなたならどうしますか？



社長？

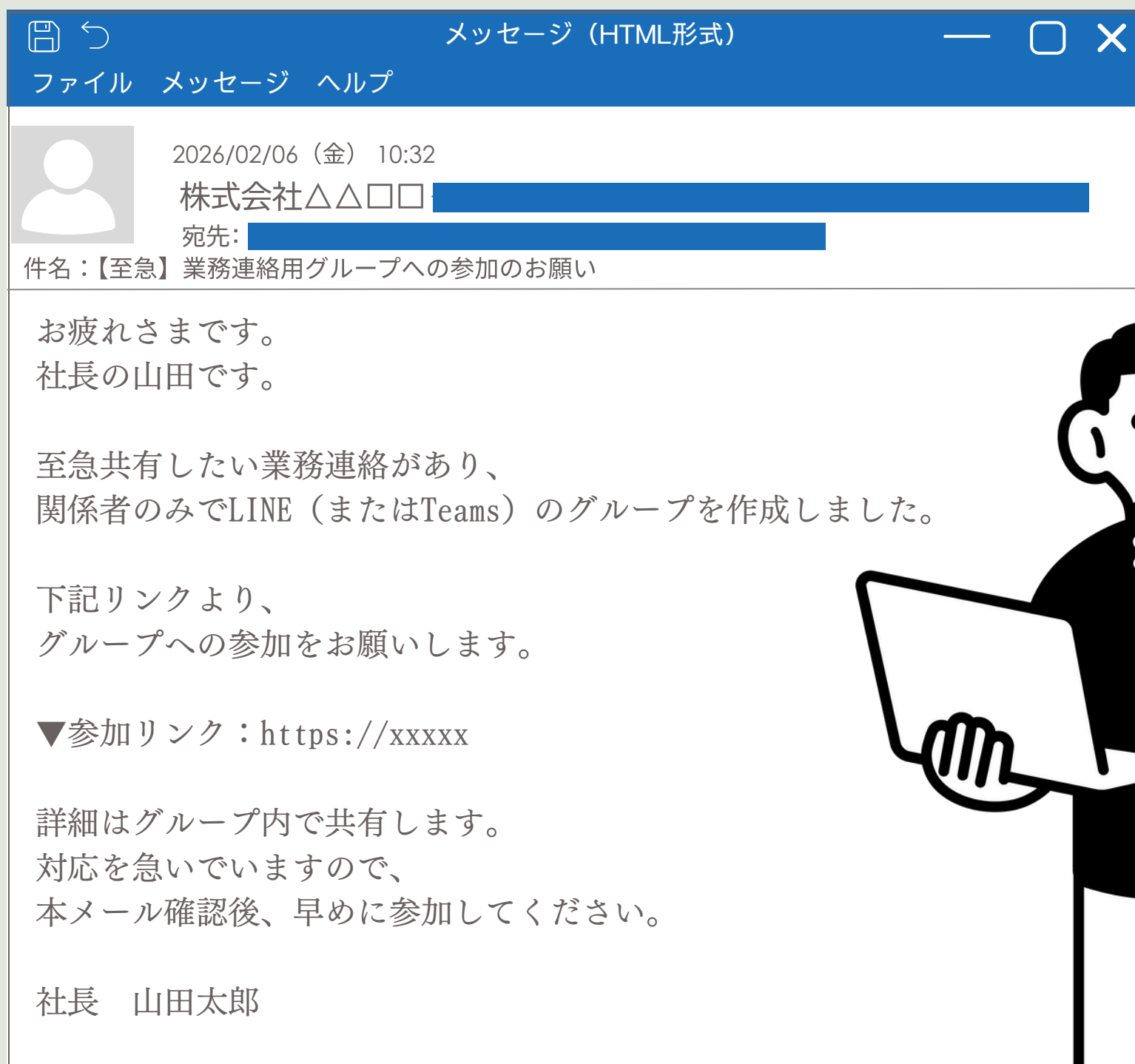


あ、社長からだ!!
急いで対応しないと!!

2. 社長名を使った「なりすまし」に注意

その判断、実は「攻撃の入口」かもしれません

社長名のメールで案内された「業務連絡グループ」に参加したあと、攻撃は始まります



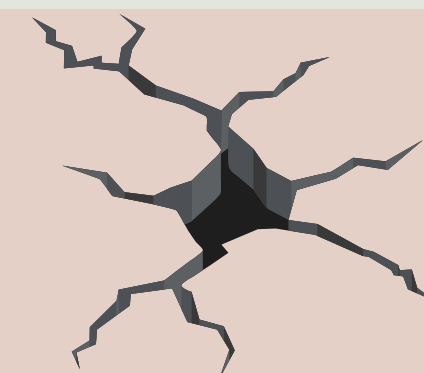
実は、「業務連絡グループに参加したあと」が本当の罠です
この手口の怖い点は、
「参加した瞬間」ではなく、
「参加してから」疑いにくくなることです。

なぜなら…

- すでに複数人が参加しているように見える
- ダミーアカウントが「了解しました」「対応します」などと反応する
- 「自分だけ疑うのは失礼かも」という心理が働く
- 社長・役員名義だと、確認をためらってしまう

攻撃の狙い

1. 社内情報の聞き出し
2. 他社員へのなりすまし拡大
3. マルウェア付きファイルの共有
4. 不正送金・請求書詐欺への発展

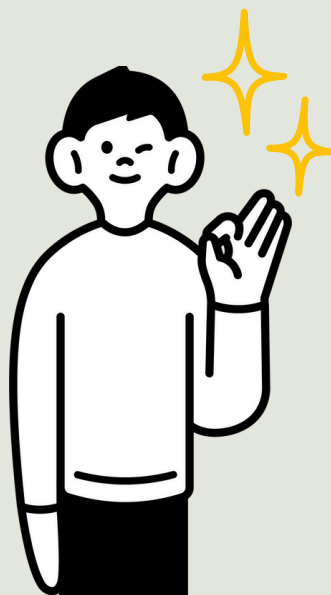


「知っている名前」ほど、確認する。
それが、今の時代の業務上の基本動作です。

2. 社長名を使った「なりすまし」に注意

理解度チェック

- ☐ 社長名のメールでも、「業務指示＝本物」とは限らない
- ☐ なりすましの本当の危険は、「参加したあと」にある
- ☐ グループ内の反応（了解しました等）が、ダミーかも知れない
- ☐ 自分だけで抱えず、管理部門に相談する



小さな確認が、大きな事故を防ぎます。

3. 選挙後に増える「便乗した連絡」に注意

選挙は終わりました。
でも、攻撃は終わっていません。



3. 選挙後に増える「便乗した連絡」に注意

実際に起きています。選挙後に増える「便乗した連絡」被害



「全社員向け」を装った“業務連絡型”リンク詐欺

■ よくある便乗メールのパターン

「選挙後の社内対応方針を共有します」

「選挙に関連した全社員向け資料です」

といった件名・文面のメールが送られ、記載されたリンクをクリックすると、社内システムを装った偽画面に誘導され、ID／パスワードを入力させられます。

選挙直後という「現実には起きている出来事」を理由にした連絡は、「ありそう」「自分も関係あるかも」と感じやすく、警戒心が下がりがちになります。

■ 対策・注意点

- ① 「全社員向け」「共有」という言葉でも、すぐに開かない
- ② リンク先でID／パスワード入力を求められたら要注意
- ③ 少しでも違和感があれば、別の手段で確認・相談する

3. 選挙後に増える「便乗した連絡」に注意

今回の学びを確認しましょう！

☒ 理解度チェック

- ☐ 「全社員向け」「共有」でも、すぐに開かない
- ☐ リンク先でID／パスワード入力には要注意
- ☐ 違和感があれば、別手段で確認する

知っているだけで、防げる攻撃があります

