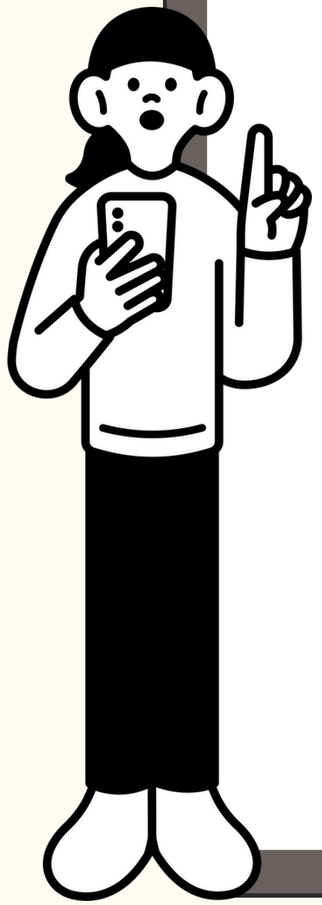
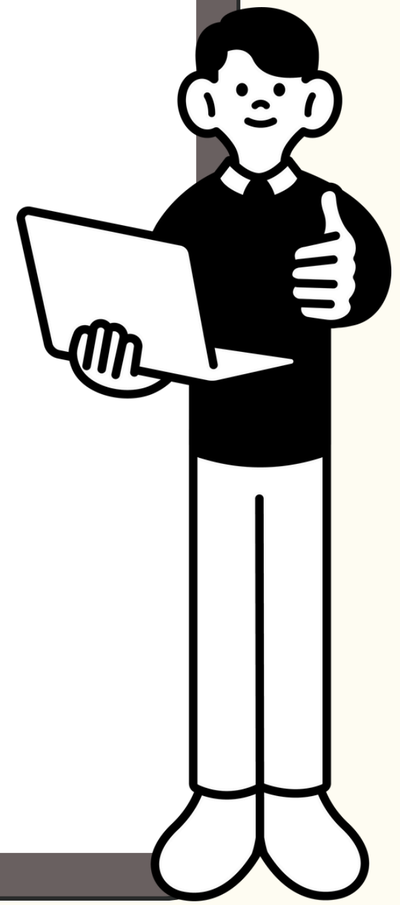


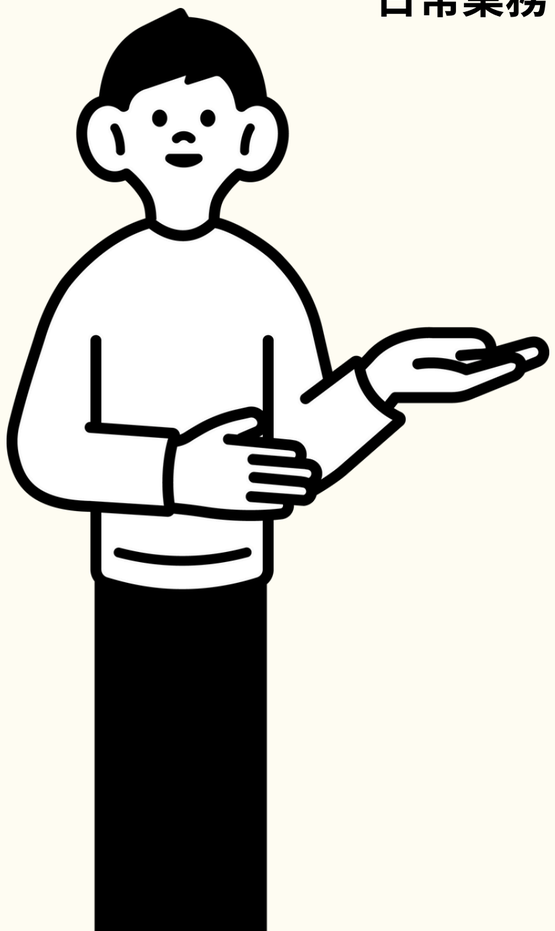
docomo Solutions

セキュリティ教育通信
2025年 11月号

NTTドコモソリューションズ株式会社



11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
無断インストールが攻撃の入口に！

2 インターネットの脅威｜Online Threats
止まるシステム、止まる業務。
日本でも広がるサイバー攻撃。

3 季節・社会動向の注意点｜Seasonal Security
還付金・年末調整を装う詐欺に注意！

１．無断インストールが攻撃の入口に！

その 便利だから は、本当に大丈夫？

１．無断インストールが攻撃の入口に！

偽フリーソフト・無断で追加した拡張機能が攻撃の入口に！

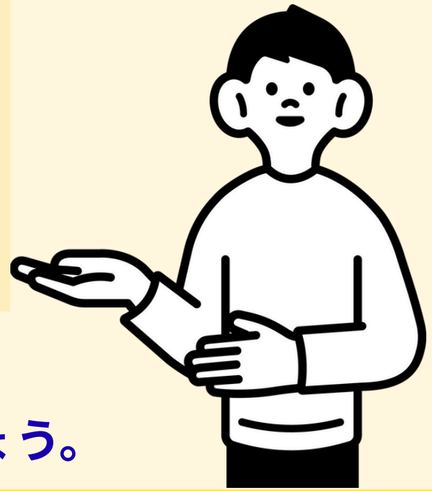
■ 報告事例

「PDF変換」「動画ダウンロード」などを装った**偽フリーソフトにマルウェア**が仕込まれていたり、
Google Chrome等の**拡張機能の無断追加**により**認証情報の窃取や端末乗っ取りに至る被害**が確認されています。

便利そうなアプリや拡張機能でも、インストールが社内への侵入口になることがあります。

■ 対策・注意点

- 業務PCには**必須以外のソフトや拡張機能を入れない**
- 利用が必要な場合は**必ず申請・承認を経て導入**
- **不要な拡張機能は削除**
- **異変に気づいたらすぐに報告**

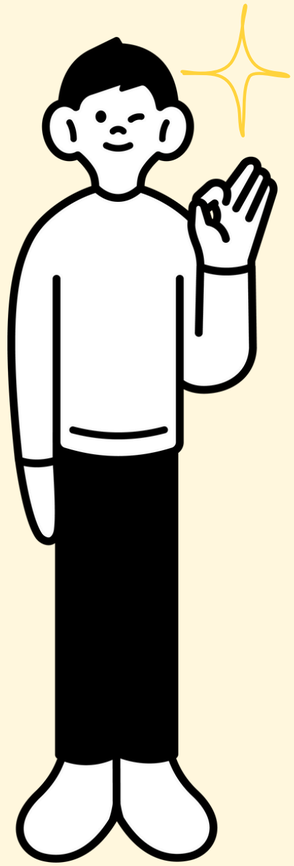


無断インストールは攻撃の入口。
インストール前に必ずひと呼吸、そして承認を経て利用しましょう。

１．無断インストールが攻撃の入口に！

☑ 理解度チェック！インストール前に確認できていますか？

- □ 業務PCに勝手にソフトや拡張機能を入れていない
- □ 新しいソフトを入れるときは申請・承認を経て導入している
- □ 使わなくなった拡張機能は削除している
- □ 「便利そう」「無料だから」という理由で自己判断していない



２．止まるシステム、止まる業務。日本でも広がるサイバー攻撃。

日本は、13秒に１回※
サイバー攻撃を受けています！

日本は世界でも有数の安全な国。
けれど、インターネットの世界では違います。
いまや日本でも、13秒に1回のペースで攻撃が観測され、
企業のシステムが“人質”に取られる事件が相次いでいます。

※出典：国立研究開発法人情報通信研究機構 NICTER 観測レポート2024（サイバー攻撃と疑われるパケット数は各IPアドレスに対して約13秒に1回観測されたことに相当）

２．止まるシステム、止まる業務。日本でも広がるサイバー攻撃。

攻撃者は、ランサムウェア（身代金ウイルス）に感染させて企業の情報を人質にします。
暗号化前のデータを搾取 → 暗号化 → 身代金要求。未払いならデータを流出する二段階手口です。
この流れで、日々の業務が止まってしまうのです。

感染・搾取

データの暗号化

身代金を要求

①金を払えば復旧してやる！
→暗号化しているデータが人質

②払わなければ全部公開する
→事前に搾取したデータが人質

二段階で脅迫

２．止まるシステム、止まる業務。日本でも広がるサイバー攻撃。

攻撃者は“人”を突破口にしてきますので、３つの心得を意識しましょう！

3つの心得

❶ 開かない

■攻撃者の狙い：偽メール・請求書・更新案内など“日常”を装う

■ポイント：**・送信元・文面を確認する。**

・「至急」「請求」「確認」など焦らせる文言は一呼吸おく

❷ 焦らない

■攻撃者の狙い：感情（焦り・信頼・得したい気持ち）を利用

■ポイント：**・感情が動いたときこそ立ち止まる**

・「ちょっと変だな」と思ったら開かない

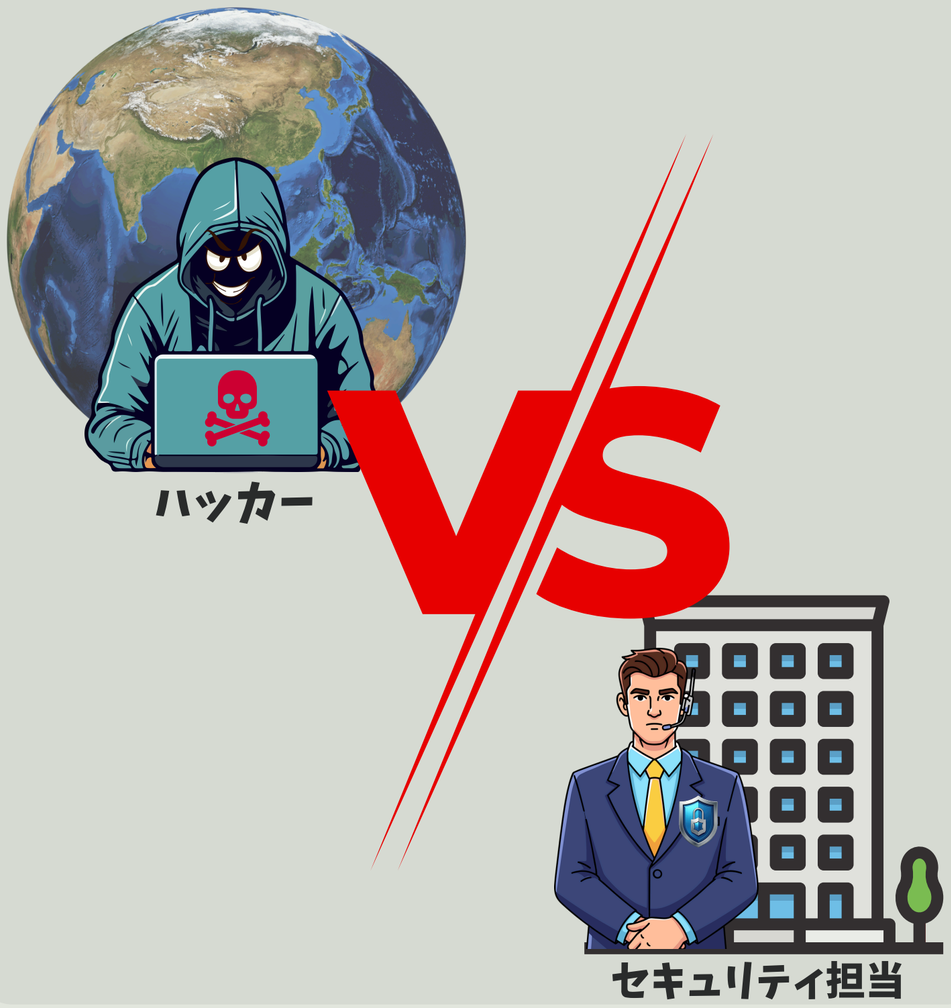
❸ 報告する

■攻撃者の狙い：感染を隠す心理を突いて被害拡大

■ポイント：**・違和感を覚えたらすぐ報告・共有**

・「自分のせいかも」と思わず早期対応を

２．止まるシステム、止まる業務。日本でも広がるサイバー攻撃。



守ってくれている人がいる。
だから、私たちも守る。

皆さんの会社のセキュリティ担当者は、
日々システムを守るためにセキュリティ対策を整えています。

それでも、攻撃者は“人”を突破口にしようとします。

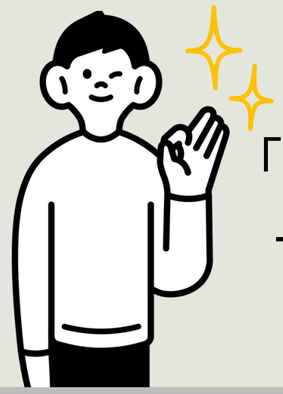
だからこそ――

社員一人ひとりの判断と行動が、
企業全体を守るための最後の防御線となるのです。

２．止まるシステム、止まる業務。日本でも広がるサイバー攻撃。

あなたのサイバー攻撃 対応力をチェック！

- □ 不審なメールや添付ファイルは開く前に送信元を確認している
- □ 「請求」「至急」「更新」などの言葉があるメールは一呼吸おいて確認している
- □ 少しでも違和感を覚えたら、すぐに上長やセキュリティ担当者に報告している
- □ 社内で共有されたセキュリティ情報に必ず目を通している



「守るのはセキュリティ担当者だけではありません。」
一人ひとりの“気づき”が、被害を防ぐ最前線です。

３．還付金・年末調整を装う詐欺に注意！

年末調整や還付金の案内が届くこの時期――

毎年11月から12月にかけて、還付金や年末調整関連を装った偽の通知が急増しています。

３．還付金・年末調整を装う詐欺に注意！

なぜ毎年、還付金詐欺等の被害がなくならないのか？

毎年被害が増える理由は…

- 「税金」「還付金」という言葉に安心してしまう
- 年1回の手続きなので慣れておらず、戸惑いやすい
- 「期限が迫る」など急かされると冷静さを失う

だからこそ、意識すべきは…

- “本当に公式からの案内か” を一呼吸おいて確認
- リンクや添付ではなく、必ず公式サイト・正規ルートで手続き
- 不安なら担当部署へ相談する

３．還付金・年末調整を装う詐欺に注意！

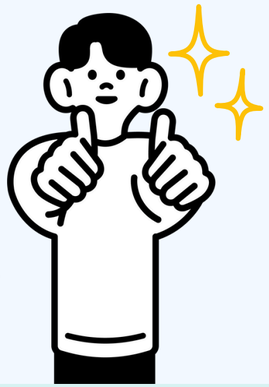
☑ 還付金詐欺等にだまされないために

□ “至急対応してください”“本日中に”と急かす通知は詐欺の可能性がある

□ 年1回の手続きだからこそ、必ず公式ルートで確認することが大切

□ “お金が戻る”という言葉に飛びつかず、一呼吸おいて確認することが大切

□ 社員一人の冷静な判断が、被害防止につながる



焦らず確認することが、最大のセキュリティ対策です。