新入社員　フォローアップ研修　2日目

若手社員のための
生成AI活用講座

知る・試す・考える。生成AIと上手につきあう3時間。



2026年10月29日（木）｜十日町商工会議所

河合 里美 ｜ トラストラボ株式会社　代表取締役

講師



河合 里美

TRUST LAB

トラストラボ株式会社　代表取締役

特定非営利活動法人 新潟県ITコーディネータ協会

新潟県ITコーディネータ協会　理事（広報）

主な支援領域

- DX認定取得支援
- 生成AI活用・研修
- Web運用・内製化

ご相談窓口

にいがた産業創造機構（NICO）DX総合相談窓口

にいがた産業創造機構（NICO）NICO 専門家派遣

ITコーディネータ

NICO登録専門家

上級ウェブ解析士（2015）

JDLA Deep Learning for GENERAL 2024 #2

G検定取得

生成AIセミナー

DX認定

ITCA DX認定サポーター
建設業２社認定実績

自社DX認定取得

トラストラボ株式会社　2025年9月1日認定
認定番号：DX-2025-09-0006-01

アジェンダ

知る → 理解する → 試す → 考える

今日は「安全に使う」から「実際に仕事で使う」までを体験します

1

緊急企画
セキュリティ

フィッシング・情報漏えい
パスワード・MFA・パスキー

自分と会社を守る

2

生成AIの基本と安全利用

生成AIのしくみ・使い分け
安全な使い方・社内ルール

AIを正しく理解する

3

生成AI活用デモ

資料を根拠に整理する方法
実際の業務活用例

まず使ってみる

4

AI企画チャレンジ

チームで企画 → 発表
AIと人の役割を考える

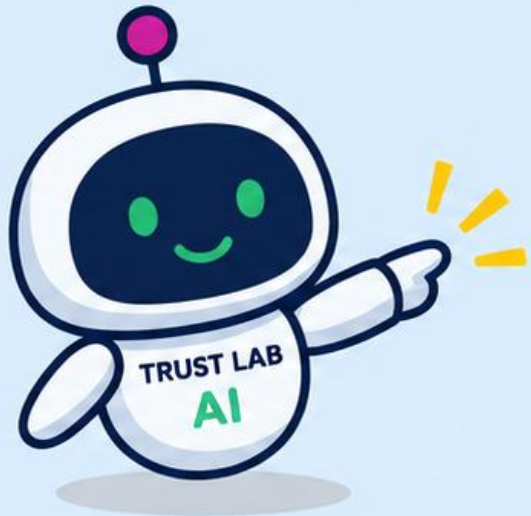
仕事での使い方を体験

本日の資料はこちらから
プロンプトもコピペできます

https://trustlab.jp/wakate_ai_cci

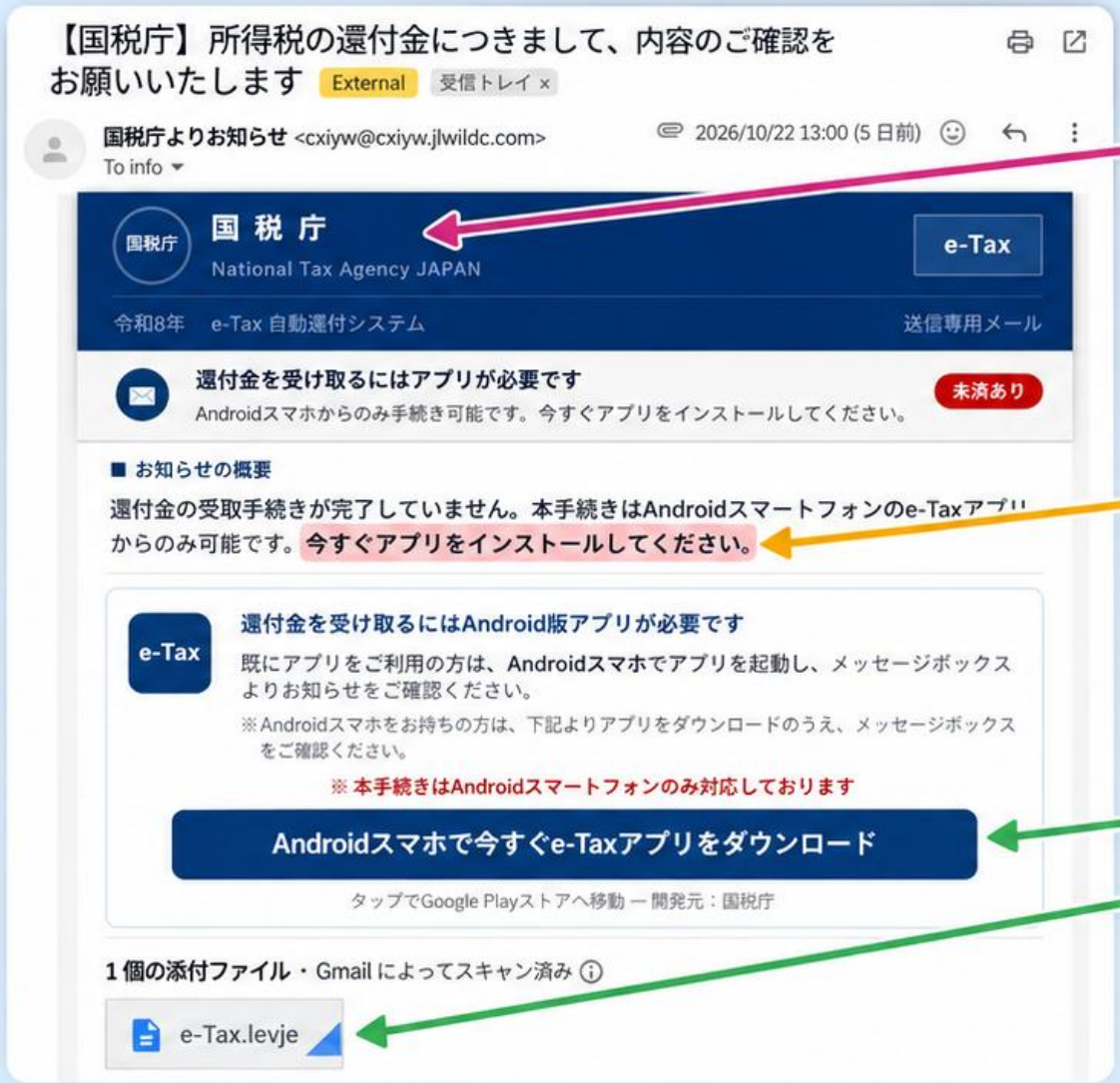
フィッシング詐欺とは？

TRUST LAB



フィッシング詐欺

実在する企業や官公庁を装った
メール・SMS・SNSなどで、
偽サイトや不正なファイルへ誘導し、
ID・パスワード、カード情報、
個人情報などをだまし取る手口です。



1 実在する機関を装う

国税庁・e-Taxを名乗って
安心させる

2 急がせて行動させる

「今すぐ」「未完了」などで
不安をあおる

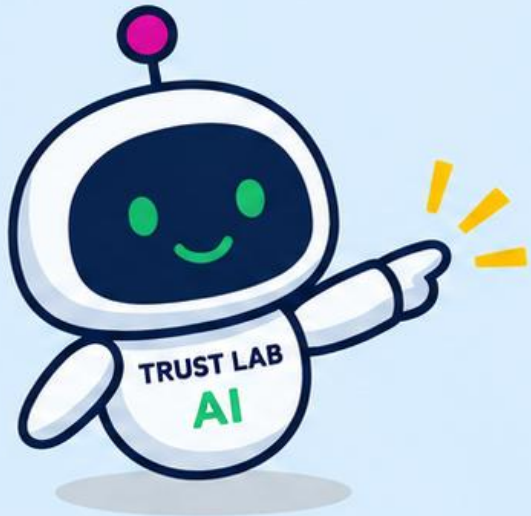
3 リンクや添付へ誘導する

ボタンや添付ファイルから
偽サイト・不正ファイルへ誘導

“本物そっくり”に見せかけて、あわてて押させるのがフィッシング詐欺です。

ランサムウェア攻撃とは？

TRUST LAB



ランサムウェア攻撃

会社や個人のパソコン・
サーバーへ侵入し、
ファイルを勝手に暗号化したり、
データを持ち出したうえで、
復旧や非公開と引き換えに
金銭を要求する攻撃です。



1 侵入して広がる

メールの添付・不正なリンク・
脆弱性などから社内へ侵入

2 ファイルを使えなくする

文書や共有データを暗号化し、
業務を止めてしまう

3 金銭や情報で脅す

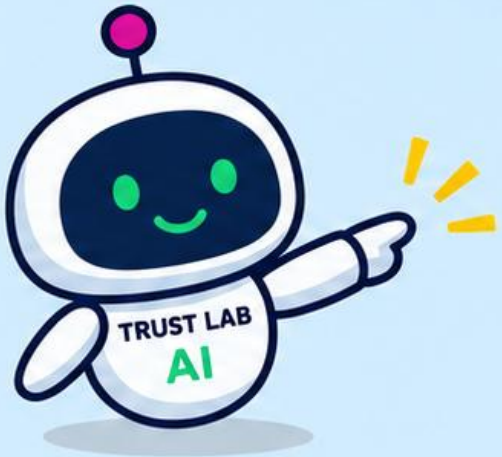
復旧費用を要求したり、
盗んだ情報の公開をほのめかす

“データを人質にして、業務を止め、金銭を要求する”のがランサムウェア攻撃です。

最近、情報漏えいが相次いでいます

TRUST LAB

2026年10月14日　国家サイバー統括室も「幅広い分野で漏えい事案が相次いで発生」と注意喚起



情報漏えい

企業やサービスが不正アクセスを受け、
氏名・住所・メールアドレス・会員情報などが外部へ持ち出されたり、第三者に見られたりする事故です。

9/28



タイムズカー

約660万アカウント

不正アクセスで会員情報が漏えい

10/8



ローソンID

215万5,345件

氏名・住所・電話番号など

10/14



infoQ

89万4,082件

個人情報を外部へ持ち出し

611件のポイント不正交換も確認

10/22



CAPCOM ID

1,177万4,247件

メールアドレス等が漏えい

196アカウントでPW不正変更

業種を選ばず発生

カーシェア・小売・Webサービス・ゲーム…



自分が気をつけていても、利用先から情報が漏れることはあります。
だから「絶対に漏れない」だけでなく、「漏れても被害を広げない」考え方が必要です。

パスワードの使い回しは危険です

TRUST LAB



【何が危ない？】1つ漏れると、次々に試される



通販サイトAで漏えい

ID：tanaka@example.jp
PW：Sakura123!

会社メール	クラウド共有	ネット通販	SNS
			
社内連絡を見られる	ファイルを見られる	不正注文される	なりすまし投稿

攻撃者は、漏れたIDとパスワードを別のサービスでも自動的に試します。これを**「パスワードリスト攻撃」**といいます。

【現実に起こること】被害は自分だけで終わらない



自分
ログインできなくなる



会社
情報流出・業務停止



取引先・知人
なりすましメール・詐欺DM

【大事な考え方】 絶対に漏れない、よりも 漏れても広がらない



サービスごとに別のPW
1か所漏れても他に広がらない



MFAを設定
PWが漏れても入りにくい



できればパスキー
そもそもPWに頼りすぎない

1つ漏れても、全部を守れるようにする

一目でわかる！MFA（多要素認証）とは

TRUST LAB



【意味】本人確認を2つ以上で行う仕組み

知識



パスワード・暗証番号

＋

所有



スマホ・認証アプリ・セキュリティキー

＋

生体



指紋・顔

この中から2種類以上を組み合わせる ＝ MFA

【どう守る？】パスワードが漏れても、1つだけでは入れない



PWが漏れた



ID・PW入力



承認・コード入力



不正ログインを防ぎやすい

たとえPWが知られても、
スマホ確認などが必要になります。

【身近な例】よくあるMFAの形

パスワード ＋ SMSコード



パスワード ＋ 認証アプリ



パスワード ＋ 指紋・顔認証

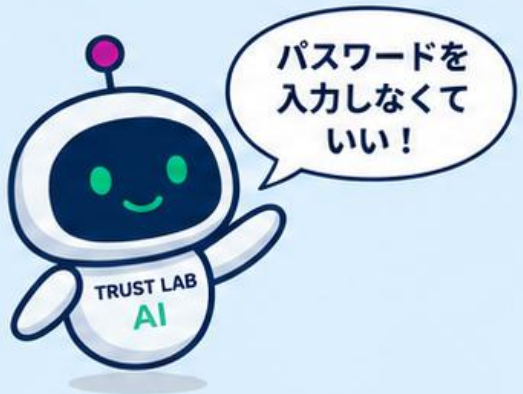


💡 **MFAは『もう1つ確認する』ことで、不正ログインを防ぎやすくする仕組みです**

一目でわかる！パスキーとは

TRUST LAB

【意味】パスワードの代わりに使う新しいログイン方法



パスワードを入力せず、スマホやPCで本人確認してログインします。

パスワード不要



本人確認



指紋・顔認証・端末のPIN など

使うもの



端末（スマホ）　端末（PC）

【仕組み】偽サイトに強く、安全にログイン

1 サービスにログイン

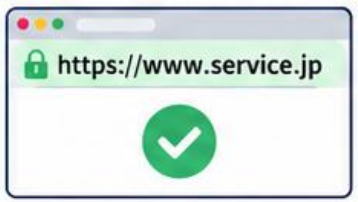


2 端末で本人確認



指紋・顔認証・端末のPIN

3 正しいサイトにだけ認証



4 ログイン完了



パスワードを
入力する必要がないため、
偽サイトにだまされにくく
安全です。



【強み】パスキーのメリット



パスワードを覚えなくてよい

複雑なパスワードを考えたり、
忘れたりする心配がなくなります。



偽サイトにだまされにくい

パスワードを入力しないため、
偽サイトで情報を盗まれるリスクを減らせます。



ログインがかんたんで速い

端末で本人確認するだけで、
すぐにログインできます。

身近な例



パスキーは『パスワードを入力しない』ことで、安全性と使いやすさを高める仕組みです

結局、何を気をつければいい？

一目でわかる！オンライン安全対策の基本まとめ

TRUST LAB



大事なのは
「だまされない」と
「被害を広げない」

【まとめ】今日から守る6つの基本

1 メールのリンクを押さない



公式アプリ・ブックマークからアクセス

2 怪しい添付は開かない



急がせる文面や見知らぬファイルに注意

3 パスワードを使い回さない



1か所漏れても被害を広げない

4 MFAを設定する



パスワードだけでは入れないようにする

5 パスキーがあれば使う



パスワードに頼らない安全なログインへ

6 迷ったら確認・報告



一人で判断せず、周囲や担当者に相談

完全に防ぐことは難しい。だから、日々の習慣と仕組みで会社と自分を守ろう！

TRUST LAB

一目でわかる！

生成AIを安全に使う5つの基本



生成AIはとても便利なツールです。正しく使えば、仕事の効率が上がります。
しかし、使い方を誤ると「情報漏えい」「誤った情報」「著作権の問題」「不正利用」などのリスクがあります。

1 機密情報・個人情報を入力しない

顧客情報
社員情報
未公開資料
パスワード
など



会社の許可なく、業務データや社内資料、顧客情報、個人情報などを生成AIに入力しないでください。

職場で契約していないAIサービスを個人的に使って業務利用すること（シャドーAI）も情報漏えいの原因になります。

2 AIの答えをそのまま信じない



生成AIは、事実と異なる情報をもっともらしく生成すること（ハルシネーション）があります。
重要な情報は必ず他の情報源で確認しましょう。

3 著作権・権利関係に注意する



生成AIが作った文章・画像・音楽などにも、著作権や利用ルールがあります。
そのまま使ってよいとは限りません。
商用利用や社外公開の前に、会社のルールを確認しましょう。

4 不正利用・攻撃にも注意する



生成AIは便利な一方で、詐欺メールの作成、偽情報の拡散、マルウェアの開発など悪用されるリスクも高まっています。
不審な指示やファイルには注意しましょう。

5 最終判断は必ず人が行う



生成AIは強力なアシスタントですが、会社固有の事情や取引先との関係、法的な判断まではできません。
AIの提案をもとに、必ず人が確認・判断して利用しましょう。

ルールを守って、生成AIを「安全に・賢く」活用しましょう！

便利さとリスクはセットです。
正しい使い方が大切です。

一目でわかる！生成AIのしくみ

TRUST LAB



【しくみ】AIは「次に来そうな言葉」を予測している

1 たくさんの文章を学ぶ



インターネット上のブログ・ニュース・書籍など、たくさんの文章から、言葉の使い方やつながりを学んでいます。

2 質問を受け取る



ユーザーからの質問やお願いなど、文章（言葉）を受け取ります。

3 次に来そうな言葉を予測



これまでに学んだ文章の中から、「この後に来そうな言葉」を予測します。

4 予測をくり返して文章にする



予測を１つずつくり返しながら、自然な文章になるようにつなげて答えを作ります。

生成AIは、「正解を知っている先生」というより、「言葉の流れを読んで答える、とても優秀な壁打ち相手」です。

【得意】こんなことは得意



文章を整える

誤字脱字の修正や
わかりやすい表現にする



アイデアを出す

企画のアイデアや
考えのヒントを提案する



要点をまとめる

長い文章をわかりやすく
整理して要約する

【注意】だから間違えることもある



もっともらしく間違う

自然な文章でも、
事実と異なる内容を
答えることがある



同じ質問でも少し変わる

毎回少しずつ
違う答えになることがある



事実確認が必要

生成AIの答えは必ず
他の情報で確認する
ことが大切

AIが準備し、人が確認・判断する

RAG・学習オフ・学習オンの違い

TRUST LAB



入力 質問・文章・画像など



RAG（資料を見ながら答える）

1 資料登録 → 2 探す → 3 答える → 4 出典確認



社内資料などを登録 → 登録資料から探す → 資料をもとに回答 → 出典を確認できる

登録資料をもとに回答

社内資料の検索・要約・確認に効果的

一般的な生成AI（学習オフ）

1 入力 → 2 回答 → 3 学習に使わない



質問・文章・画像などを入力 → AIが回答を生成 → 入力内容はモデルの学習に使われない

下書き・相談に使いやすい

一般的な生成AI（学習オン）

1 入力 → 2 集める → 3 学習 → 4 次に活かす



質問・文章・画像などを入力 → 多くのユーザーの入力を集める → 集めたデータでモデルが学習・改善 → よりよい回答や機能に活かされる

精度向上・機能改善のイメージ

一目でわかる！ 主要な生成 AI の使い分け

TRUST LAB



AI は
使い分け！

【使い分け】どれが一番ではなく、「仕事の種類」で選ぶ

C ChatGPT

相談・思考・作成

質問・文章作成・アイデア出し
調査・ファイル分析・データ分析

万能型の相談相手

W ChatGPT Work

エージェント

調査→分析→資料作成
複数ファイル・アプリをまたぐ仕事

仕事を任せて完成まで進める

G Gemini

相談＋エージェント

調査・文章／画像生成
Google サービスとの連携

Google と一緒に働く AI

N Gemini Notebook

資料ベースの相談・研究

手元資料をもとに質問
要約・比較・レポート・音声化

「この資料をもとに」が得意

A Claude

相談・作成＋エージェント

長い文書の読解・文章・分析
コード・複数ステップ作業

深く考えて、形にする AI

M Microsoft Copilot

業務統合＋エージェント

Word ・ Excel ・ PowerPoint
Outlook ・ Teams 上の仕事

Microsoft 365 の中で働く AI

生成 AI は「名前」ではなく、やりたい仕事に合わせて選ぶと使いやすい。

✓ 【使い分け】こんな時はこれ

相談 → ChatGPT / Gemini / Claude

資料 → Gemini Notebook

仕事を進める → Work ・ エージェント系

! 【注意】会社で使うとき

「自分の好きな AI」ではなく、
会社が許可した AI を使う。

💡 AI は名前で選ぶのではなく、仕事で選ぶ

生成AIガイドライン、どう作る？

TRUST LAB

【基本】 国の資料を土台に、自社で迷わないルールへ



生成AIガイドライン

会社でAIを安全に使うための「利用ルール」です。
ゼロから作らず、国の資料やひな形を参考に、自社の業務に合わせて整えます。

まず、国の資料を“土台”にする

経 経産省

AI事業者ガイドライン
第1.2版

▶ 全体方針・基本原則

I IPA

テキスト生成AIの
導入・運用ガイドライン

▶ 導入・運用・リスク管理

デ デジタル庁

生成AIの調達・利活用
ガイドライン 第2.0版

▶ ひな形・チェックシート

個 個人情報保護委員会

生成AIサービス利用の
注意喚起

▶ 個人情報の扱い

1 必要な項目を拾う

国の資料から、自社に必要な
考え方・項目を選ぶ

2 自社の業務に置き換える

使うAI・入力情報・確認方法を
自社の仕事に合わせる

3 A4一枚のルールへ

現場が迷わず使える形にして
使いながら見直す

“国の資料をコピーする”のではなく、自社で「迷わず使えるルール」にする。

参考：経済産業省／IPA／デジタル庁／個人情報保護委員会（2026年10月確認）

Gemini Notebookで生成AIガイドラインを作る

TRUST LAB



【考え方】 AIにゼロから規程を書かせず、信頼できる資料を「整理」させる

1 国の公式資料を集める
経産省・IPA
デジタル庁・PPC

2 Gemini Notebookへ入れる
PDF・Web・
Googleファイル

3 共通ポイントを整理する
根拠を示しながら
比較・要約

4 自社向けA4ルール案に変換
使うAI・入力情報・
確認方法を自社向けに

5 人が確認・決定
承認・相談先・
見直しまで決める

デモで入力

① 「4つの資料を確認し、業務利用で共通して注意すべき事項を整理。
各項目の根拠となる資料も示してください。」

② 「自社の条件を加え、社員が迷わず守れるA4一枚のルール案に。
重要なものを5つに絞ってください。」

ここが重要！

AIが作ったものは「案」。

会社の事情・情報管理・承認ルールは
最後に人が確認して決める。

国の資料 → AIで整理 → 自社向けに変換 → 人が確認・判断

参考：Google公式ヘルプ／経産省／IPA／デジタル庁／個人情報保護委員会（2026年10月確認）

デモ　商品の魅力を、外国人にも伝わる接客ツールに変える



TRUST LAB

1 商品情報を入力



お店の商品について
簡単に入力します。

2 AIが外国語に翻訳



ChatGPTにお願いして、
わかりやすく自然な
外国語に翻訳します。

3 言語別再生ボタン選択ウェブサイト作成



翻訳した内容を使って、
言語別の再生ボタンが選べる
接客用のウェブサイトを作成します。

4 外国人観光客へ案内（お店で使う）



QRコードを設置すれば、
お客様が自分で言語を選んで
音声で案内を聞くことができます。

今回のデモで使うツール

ChatGPT で翻訳

Clipchamp で無料の音声生成
https://app.clipchamp.com/consumer/home

ワークショップ　AI企画チャレンジ！

～ 雪国地域に20代・30代を呼び込むPRイベントを企画しよう ～



【MISSION】 あなたは「若手企画チーム」。生成AIを使って“通る企画”を作る！

チームで決める5つ

1. **イベント名**
   覚えやすく伝わる名前
2. **キャッチコピー**
   行きたくなるひと言
3. **企画内容**
   何を体験できるイベント？
4. **SNS告知**
   誰に・どこで・どう伝える？
5. **告知写真 1点**
   ネット検索OK 実際に選ぶ

今回の仕事

雪国地域に20代・30代の人を呼び込む、新しい地域PRイベントを考えてください。

生成AIは自由に使ってOK

- ✓ 分からないことは「上司役」に相談OK
- ⏱ 企画時間：約15分
- 発 最後に2分プレゼン

発表では「なぜこの企画にしたのか」「なぜこの写真を選んだのか」も説明してください。

AIをうまく使って、「これは通るだろう」という企画を作ってみよう！