論点2

AI利活用のための
ガバナンス

町田市デジタル化推進委員会

ジェネレーティブAI（生成AI）は、メガトレンド化

技術・サービス

① イラスト、動画、音楽などを生成する専用AIの登場
② 文章・画像・音声を組み合わせて扱えるAIの登場
③ 様々なサービスへの組み込みが進んでいる

生成AIが扱う領域は拡大し、適用可能な業務も拡大している

生成AIを、DXツールとして活かすには?

リスク 誤情報の生成、個人情報や機密情報の漏えい、著作権侵害

ガバナンス

東京都は「文章生成AI利活用ガイドライン」を策定
神戸市などの基礎自治体においても、ガイドラインを策定
→自治体におけるChatGPTのガイドラインは、事実上標準化

町田市の状況 試行版のガイドラインを策定し運用中

生成AIは、DX推進の強力なツールとして期待される

市のこれまでの取組

2023 5月
NTTデータと連携協定を締結

8月
Azure Open AI（ChatGPT）で構築
▶ Teams ＋ Azure OpenAI Service API

9月
「AI利活用ガイドライン試行版」を策定し、試行運用を開始
▶ 全庁から200人を公募

11月
「AI利活用ガイドライン」を確定版とし、本運用を開始予定
▶ 全職員4,000人を対象

⚠ ChatGPTは、情報漏えい事故が起きるって聞いたんだけど、大丈夫なの？

一般的なChatGPT

質問内容はぜんぶ学習！
他人の回答に使っちゃうかも?!

質問 →

← 回答

ChatGPT

⚠ 世界中で同一のAIを共用

情報漏えいリスク!

町田市のChatGPT

質問は学習しないよ！

質問 →

← 回答

AzureOpenAI ＋ 公開情報

✓ 市職員専用のAIを利用

安全＆正確!

安心して！市は、対策済みの安全なChatGPTを使うよ！

「カワセミールDX」
（イラストはAIが生成）

観点1 職員が文章生成AIを利用するうえで、対策に過不足はないか？

用 途 情報のリサーチ、文章の要約、文章案の作成、言語翻訳、分類、分析など

課 題 誤情報の生成リスク、個人情報や機密情報の漏えいリスク

ガイドラインに追記すべき項目

運用面の対策

規定済の項目

- 町田市専用AI以外の利用禁止
- 町田市専用AIの業務外利用禁止
- 個人情報や機密情報の入力禁止
- ファクトチェックの徹底

試行運用等で得られた知見を追記

- AIへの命令を明確にする
- 特定の作家等に似せる指示禁止

技術面の対策

すでに実装しているものを追記

- 町田市専用AIの整備
- AIによる入力情報の学習禁止
- AIの初期化や停止が可能
- 公開情報(オープンデータ)を学習
- アクセスログを確認

観点2 職員が、画像生成AIを利用する場合の対策は？

用 途 市民・庁内向けの、表紙・挿絵などのイラスト・デザイン・ロゴ

課 題 他者の著作権等を侵害してしまうリスクがある

ガイドラインに追記すべき項目

① 著作権クリーンなAIを利用・併記

例：著作権等がないデータを
学習した画像生成AI 「Emi」

② 特定の作品等に関する指示禁止

例：「●●風にして」など、
似せる指示をしない

③ 侵害抑止機能を利用

例：権利侵害に関する指示の排除
権利侵害検知機能

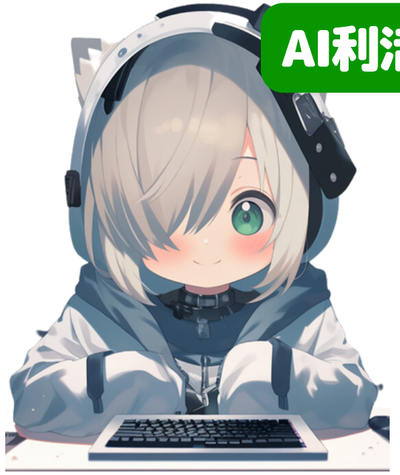
④ リスク保証型のサービスを利用

例：Microsoft 365 Copilotは、
生成AIの訴訟リスクに対応

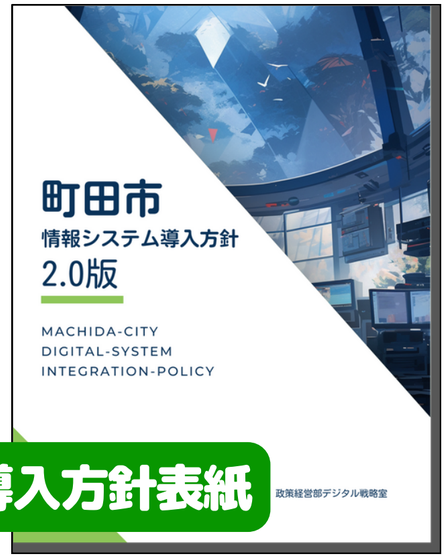
⑤ 画像を学習データとして入力しない

論点2「AI利活用のためのガバナンス」

画像生成AIの活用実例



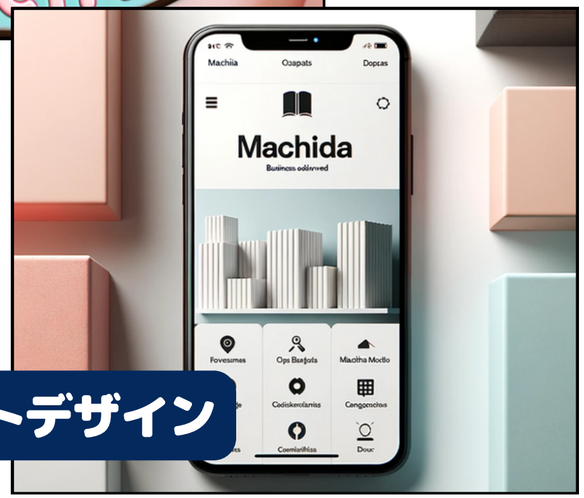
AI利活用ガイドライン挿絵



情報システム導入方針表紙

画像生成AIの活用想定

ロゴデザイン



Webサイトデザイン

観点3 サービスの一部に生成AIが組み込まれたものを、調達する場合の留意点は？

例 議事録、翻訳、音声認識、データ分析、FAQチャットボット、RPA など

課 題 生成AIの積極活用を見据えた際に、このようなサービスをどう調達すべきか定まっていない

対策案

① AI利活用ガイドラインから逸脱する場合、サービス事業者から情報セキュリティ対策の代替策を提示

② 独自利用型サービスを前提としたAI利活用ガイドラインから、共同利用型サービスを想定したガイドラインへの移行を検討

③ 当面の間、サービスを利用しない