生成AI利活用ガイドライン

ルール編

制定日：2026年5月

東京都町田市

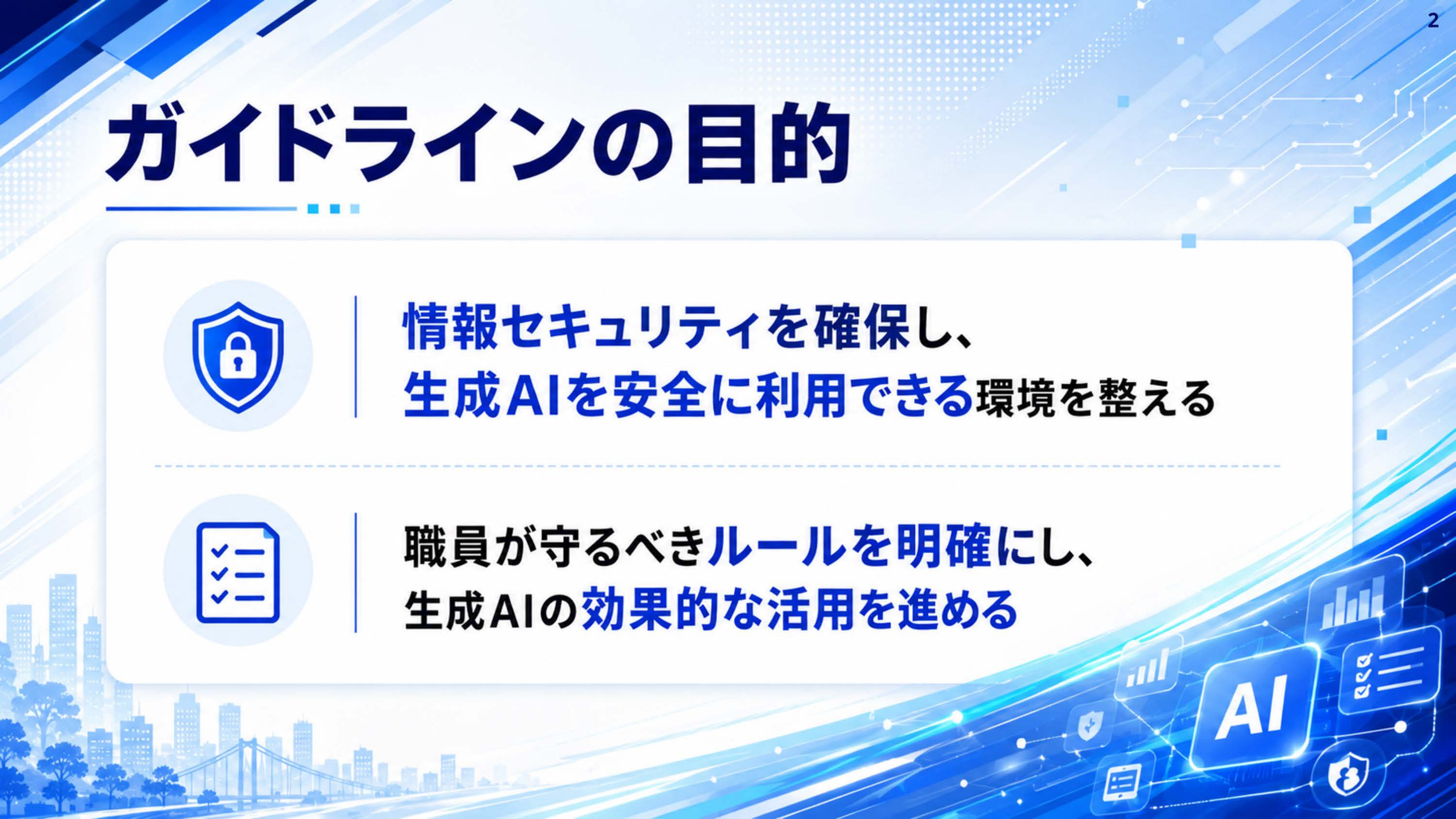
政策経営部デジタル戦略室

AI生成画像を使用

ガイドラインの目的

情報セキュリティを確保し、
生成AIを安全に利用できる環境を整える

職員が守るべきルールを明確にし、
生成AIの効果的な活用を進める



ガイドラインの適用範囲

このルール編は、『対象者』と『対象サービス』を明確に定めています。

対象者

業務で生成AIサービスを
利用する、
すべての職員

このルール編は、業務で生成AIサービスを
利用するすべての職員に適用されます。

職員が守るべき利用ルール → 7ページ

対象サービス

すべての生成AIサービス

サービスの一部に生成AIを組み込んだものを含む

このルール編は、
すべての生成AIサービスに適用されます。

生成AIを導入する際の技術的ルール → 13ページ

あわせて読む

推進編

職員用AIナビゲーター（スタッフモード）を活用するための手引き

スタッフモードで利用する主な機能の使い方と注意点

汎用AI　ナレッジAI　業務審査AI　AI利活用相談

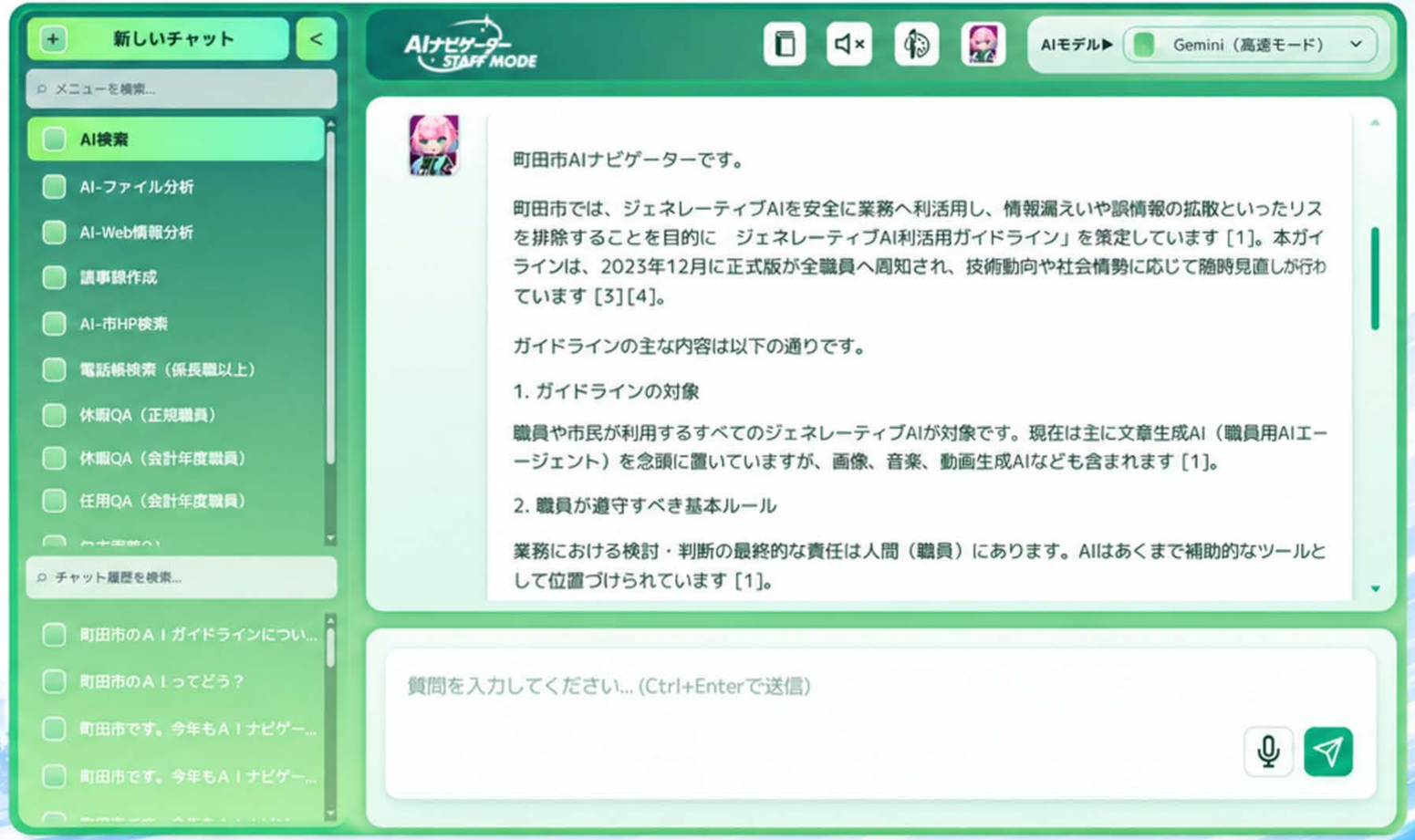
市民向けではなく、職員向けAIナビゲーターの活用ガイド

ルールを守る → スタッフモードを安全に活用する

【コラム】AIナビゲーターは、なぜ安全？

市民向けAIナビゲーター

職員向けAIナビゲーター



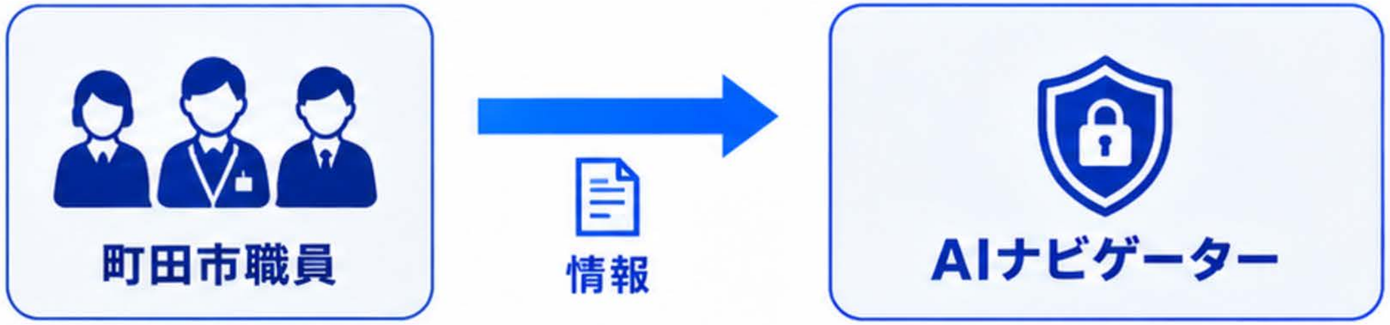
【コラム】AIナビゲーターは、なぜ安全？

一般的な生成AIサービスは…

- 不特定多数のユーザーが利用する
- 入力情報が意図せず外部で利用される
- 誰がどう利用したか確認できない
- 障害発生時のサービス停止や再開がサービス提供事業者に依存する

AIナビゲーター

- 職員のみが利用する専用環境
- 入力情報がサービス提供事業者に渡らない
- アクセスログを取得し、確認が可能
- 生成AIサービスを市の意向で開始や停止できる



生成AIサービスを安全な環境で利用することができる！

職員が守るべき利用ルール

職員が守るべき利用ルール

ルール 1

生成AIサービスでの
個人情報の扱いは、
業務に必要な**最小限**の
ものとすること

ルール 2

業務では**市が提供する**
生成AIサービスのみ**利用**し、
業務以外の目的では
利用しないこと

ルール 3

回答精度を高めるために、
生成AIサービスへの
命令を明確にすること

ルール 4

生成AIへの命令に
第三者の著作物や作家名、
作品名を**含めない**こと

ルール 5

生成物を利用する際は、
根拠や第三者著作物との
類似性を**確認する**こと

ルール 6

生成AIサービスを
安全かつ効果的に利用する
ために、**研修を受講する**こと

補足説明

ルール 1

1

生成AIサービスでの個人情報の扱いは、業務に必要な最小限のものとすること

- 生成AIサービスにおける個人情報の扱いは、個人情報ファイル簿のとおりとし、**業務に必要な最小限のもの**としてください
- 生成AIサービスを業務で利用する場合は、**デジタルサービス等導入企画書**を作成してください
- 個人の権利侵害や行政運営に重大な影響を及ぼす情報（機密性3A情報）は**入力禁止**とします

個人情報ファイル簿とは

市が保有する個人情報を含む事務について、利用目的や対象者、記録項目、保有形態、提供先等を記載した台帳です。

デジタルサービス等導入企画書とは

新たにデジタルサービス等を導入・利用する際に、目的・効果、リスク、情報の取扱い等を整理し、事前に審査・承認を受けるための企画書です。

補足説明

ルール2

業務では市が提供する生成AIサービスのみ利用し、業務以外の目的では利用しないこと

- 業務では、情報セキュリティ対策が確保されている、市が提供する生成AIサービスを利用してください
- これ以外のサービスは、不特定多数のユーザーが利用し、入力情報が意図せず外部利用される可能性があるため、業務利用は禁止です

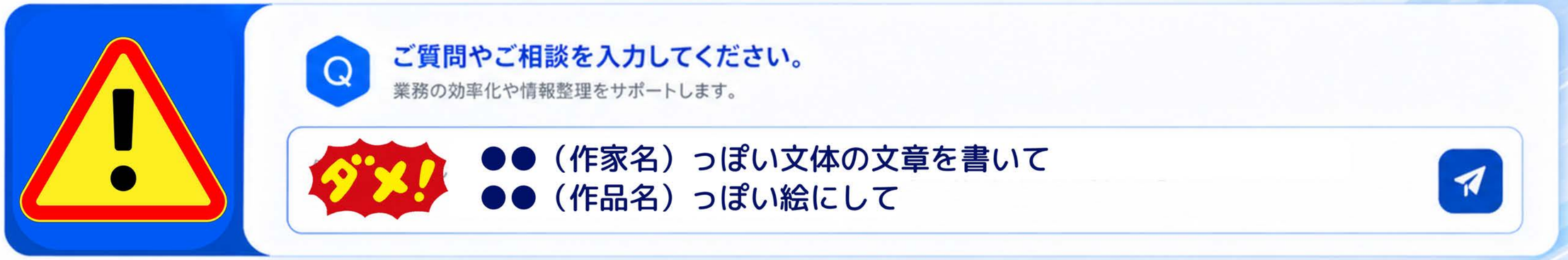
ルール3

回答精度を高めるために、生成AIサービスへの命令を明確にすること

- 生成AIに対する命令が曖昧だと、誤った情報を生成してしまう恐れがあります
- 伝わりやすい日本語を心掛け、解釈の余地がある表現は避けて命令してください

補足説明

ルール4　生成AIへの命令に第三者の著作物や作家名、作品名を含めないこと



著作権等を侵害しないために、生成AIを利用する際、特定の作品名や作家名を指定しないでください

第三者の画像や文章等の著作物を、生成AIへの命令に含めないでください

補足説明

ルール 5

生成物を利用する際は、根拠や第三者著作物との類似性を確認すること

- 生成AIは、虚偽や偏りのある回答を生成する可能性があるため、必ず根拠を確認してください
- イラスト等、創作性の高い生成物を外部に公開する場合には、生成物が既存の著作物に類似していないことを確認してください

ルール 6

生成AIサービスを安全かつ効果的に利用するために、研修を受講すること

- 生成AIの特性と「職員が守るべき利用ルール」を正しく理解し、安全かつ効果的に生成AIサービスを利用できるよう、必要な研修を受講してください

生成AIを導入する際の技術的ルール

生成AIを導入する際の技術的ルール

本市の業務に生成AIを安全・安心に導入・利用するため、以下の技術的ルールを満たすことを必須とします。

ルール 1

専用環境で
生成AIサービスを
利用できること

ルール 2

入力情報が
サービス提供事業者に
渡らない生成AIサービスを
利用すること

ルール 3

市の意向で
生成AIサービスの
開始や停止が
できること

ルール 4

生成AIサービスの
アクセスログを**取得**し、
確認できること

ルール 5

生成AIサービスへの
サイバー攻撃対策が
できていること

補足説明

ルール 1

専用環境で生成AIサービスを利用すること

- 他の利用者と分離された利用環境（専用テナント等）を確保すること
- 多要素認証の仕組みを備えること
- 利用者のアクセス権限を管理できること

ルール 2

入力情報がサービス提供事業者に渡らない生成AIサービスを利用すること

- 生成AIへの命令が、学習データとしてサービス提供事業者に利用されないこと
- 生成AIへの命令及び生成物が、外部提供や二次利用されないこと

専用テナント とは

クラウドサービスにおいて、特定の組織のみが利用できる専用の環境のことです。
他の組織と論理的に分離され、独立したリソース（計算・保存領域等）を
利用できるため、セキュリティと管理性を高めることができます。

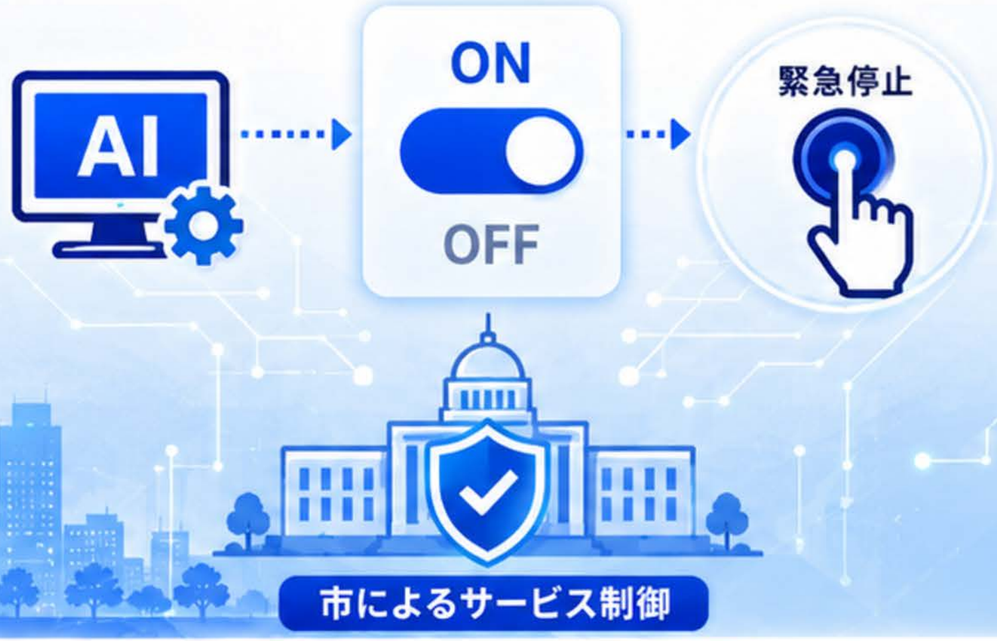
多要素認証 とは

パスワードに加えて、スマートフォンアプリやワンタイムパスワード、生体認証など、
複数の異なる要素を組み合わせて本人確認を行う仕組みのことです。
不正アクセスのリスクを大幅に低減できます。

補足説明

ルール3　市の意向で生成AIサービスの開始や停止ができること

システム障害等、不測の事態が発生した際に、
市がサービスの利用停止や再開を速やかに
実施できること



ルール4　生成AIサービスのアクセスログを取得し、確認できること

- 利用者ID、利用日時、操作内容等を記録した
  アクセスログを市が取得できること
- サービス提供事業者はアクセスログの
  改ざん防止措置を講じること

補足説明

ルール 5

5

生成AIサービスへのサイバー攻撃対策ができていること

サービス提供事業者は、
不正アクセス対策を実施すること

- WAF
- IDS/IPS
- IPアドレス制限
- 証明書認証（相互認証）

サービス提供事業者は、
脆弱性対策を実施すること

- セキュリティ診断（脆弱性診断）
- パッチ適用（アップデート管理）
- プロンプトインジェクション対策

サービス提供事業者は、
システムの監視及びシステム障害の対応体制を整えること

- システム監視（常時監視・ログ監視）
- アラート検知（早期検知）
- インシデント対応体制（24時間・エスカレーション）

不正アクセス対策とは

外部からの不正なアクセスや侵入を防ぐための対策です。WAFやIDS/IPSの導入、アクセス元の制限、強固な認証などにより、第三者による不正な利用や情報の窃取を防ぎます。

脆弱性対策とは

システムやソフトウェアの脆弱性（セキュリティ上の弱点）を早期に発見し、修正・改善するための対策です。診断の実施や、アップデート・パッチ適用等を適切に行います。