2025年度ISSスクエアシンポジウム研究成果発表

生成AIの業務活用による不適切入力のリスク

2026年2月27日
マネジメント分科会

マネジメント分科会の紹介

マネジメント分科会の研究方針

様々なルール・基準と実際の乖離に注目し、

実際のシステムや環境、予算、組織文化・人に合わせた対策を

調査・議論を通して、総合的に検討

メンバー

- リーダー：稲葉 緑 教授
- M2：町田、西村、加藤、対馬、立澤、伊藤
- M1：藤井、平瀬

目次

1. 研究テーマ

昨年度のテーマ： 内部不正とその対策に関する課題

今年度のテーマ： 生成AIの業務活用による不適切入力のリスク

https://forbesjapan.com/articles/detail/62905

https://toyokeizai.net/articles/-/918886

1. 研究テーマ

内部不正による情報の持ち出しは実行者が限られているが、
「生成AIへの不適切な入力」も情報の機密性を損なう点では同様であり
むしろ非悪意な分、誰もが当事者となっているのでは？

RQ1

「生成AIへの不適切入力」は「内部不正の持ち出し」と比較し、
どのような質的違いがあるか？その差に対する対策は？

RQ2

企業や組織で生成AIを業務活用する際に、どこに個人情報や機密情報の不適切な入力が発生するリスクがあるのか？

２．内部不正による持ち出しと生成AIへの不適切入力

共通点
内部者によるルールからの逸脱

- 外部からの攻撃ではない
  正規アクセス権や業務手段を利用した内部者による行動

- 会社・組織の情報を自分/自分の業務のために利用
  例）内部不正　　：自社の技術情報をもって転職先にアピール
  　　不適切な入力：自分で作成したコードの修正

- 結果として情報の機密性を損なう行為

2．内部不正による持ち出しと生成AIへの不適切入力

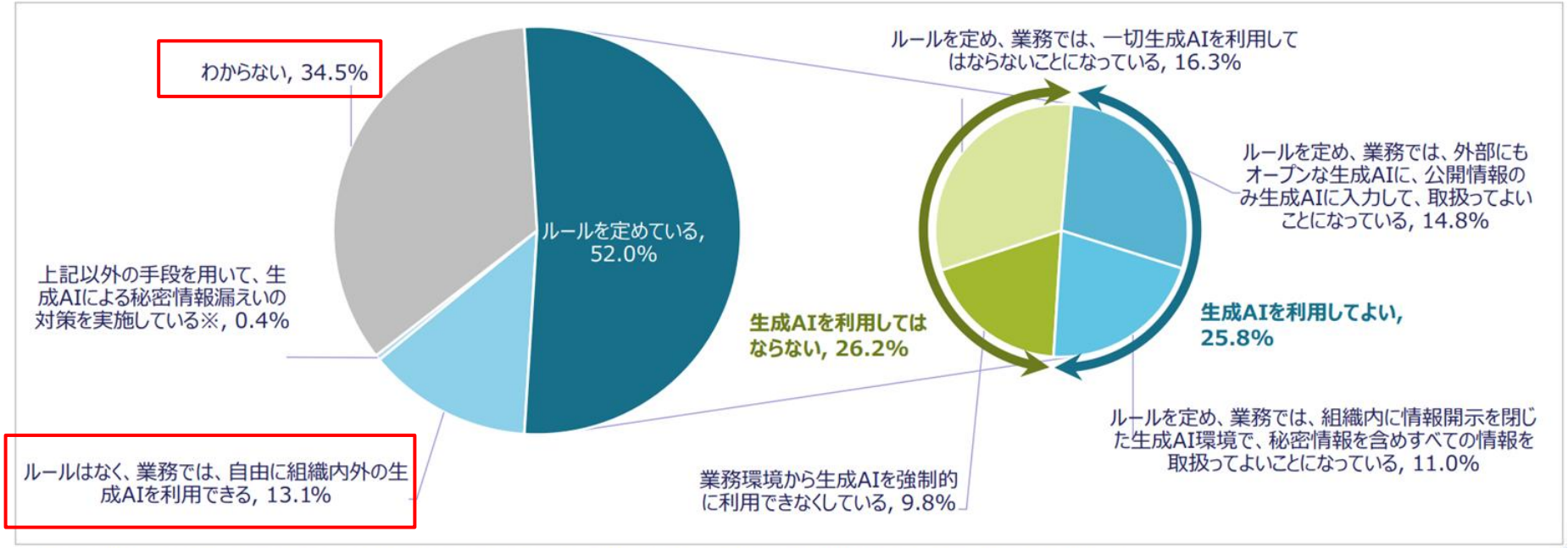
相違点
「入力」という日常行為が起点で事故化しうる

- 不適切入力は業務効率化や品質向上のためといった非悪意な動機
- 内部不正は外部へ持ち出す行為が明確、不適切入力は日常行為の延長
  例）内部不正　　：USB、メール送信、私的クラウドへアップロード
  　　不適切な入力：入力、貼り付け
- 内部不正は実行者が限られるが、不適切入力は誰もが当事者になり得る

2．内部不正による持ち出しと生成AIへの不適切入力

IPA『企業における営業秘密管理に関する実態調査2024』

「生成AI の業務利用可否と取扱い可能な情報の種別」



※印を選択した場合は自由記述欄に追記。「利用が無い」旨や、「業務情報の種別から生成AIで扱う対象ではない」等の記述があった。

https://www.ipa.go.jp/security/reports/economics/ts-kanri/j5u9nn0000004yjn-att/TradeSecret_summary_2024_r1.pdf

２．内部不正による持ち出しと生成AIへの不適切入力

対策：業務ルールの策定と利用管理、
そしてどこにリスクが発生するかの認識・教育を

- 業務ルールの作成
- **業務利用において想定される不適切入力をしてしまう場面の教育**
- 入力内容（プロンプト）の定期的な確認（監査）
- 利用可能な生成AIの事前決定と承認制
- 生成AIがどのプラグインと連携しているかの把握と承認

【参考】内部不正の対策例

- **重要情報とわかるラベル付け** ← 不適切入力でも重要
- **情報システムへのアクセス権限管理** ← 不適切入力でも重要
- 個人デバイスの持ち込み管理
- 業務利用デバイスの持ち出し管理

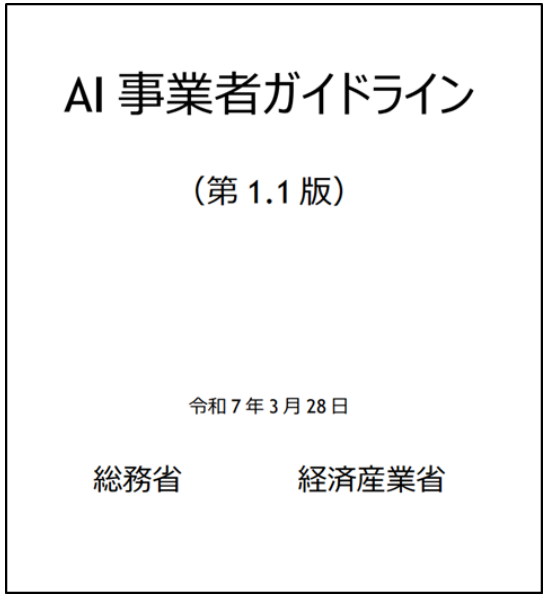
2．内部不正による持ち出しと生成AIへの不適切入力

RQ1

「生成AIへの不適切入力」は「内部不正の持ち出し」と比較し、
どのような質的違いがあるか？その差に対する対策は？

内部不正も不適切入力も、どちらも内部者による行為ではあるものの、
不適切入力は非悪意で、「入力」という日常行為が起因で発生する。
入力内容の定期的な確認や**どの業務活用にリスクが生じるか教育**が重要

３．総務省・経済産業省『AI事業者ガイドライン』



AI開発・提供・利用にあたって必要な取り組みについて、基本的な考え方を示したもの

開発者、提供者、利用者ごとに考慮すべきリスクや対応方針も記載されている

- 初版は2024年4月（2025年3月に1.1版）
- 全39ページ
- 別添にワークシート有

例）
開発者：正確性を重視するために公平性等が損なわれたりするため適宜修正が重要

提供者：開発者の意図した範囲で当該システムに実装し、運用を継続することが重要

利用者：提供者の意図した範囲で適正利用をすることが重要。また、人間の判断を介在させることも求められる。

3．総務省・経済産業省『AI事業者ガイドライン』

「AI事業者ガイドライン（第1.0版）」ワークシート（別添7）

開発者、提供者、利用者ごとに
ガイドラインに記載された内容に関する具体的なアプローチが記載

３．総務省・経済産業省『AI事業者ガイドライン』

ワークシート例）人材採用担当者　エントリーシートの活用事例

分類	検討事項	具体的なアプローチ
AIシステム・サービスに影響するセキュリティ対策	エントリーシートの入力時等に機密情報等の不適切入力に留意することが必要	データ入力時に機密情報等の不適切入力を行っていないかダブルチェックを行う
「共通の指針」の対応状況の説明	エントリーシートの情報を用いるため、申込者へ情報提供が必要	申込者に対して、データの利用範囲等について情報提供をする
多様性・包摂性の確保	情報リテラシーが十分でない応募者への配慮が必要	障がい者雇用のプログラム等、電子ファイルによるエントリーシートを作成するための情報リテラシーが十分ではない人材採用のチャネルは採用AIとは別に人事業務として用意する
人間の判断の介在	出力結果が含みうるバイアスの確認が必要	著しい学習データの不足やモデル評価への影響に開発部門で対応できないバイアス(例：外国籍の応募者、障害者雇用の対象者、従来重視していなかった職種等)について、AI開発者から説明を受け業務側でカバーできるか確認する

**機密情報の取り扱いから
バイアスまで広く記載**

４．生成AIの業務活用と不適切入力のリスク

「AI事業者ガイドライン（第1.0版）」ワークシート（別添7）の利用者例は
「人材採用担当者のエントリーシート」の活用事例のみ

RQ2

企業や組織で生成AIを業務活用する際に、どこに個人情報や機密情報の不適切な入力が発生するリスクがあるのか？

**人材採用担当者以外の一般的に存在するだろう部門における
生成AIを業務活用するシチュエーションを検討し
「機密情報」「個人情報」を入力してしまうシナリオを考えてみた**

4．生成AIの業務活用と不適切入力のリスク

「個人情報」や「機密情報」をなぜ入力してはいけないのか？

- 学習され、他の人の出力結果になるリスク
- アカウント漏洩による不正ログインでプロンプトを閲覧されるリスク
- ツールのバグで他ユーザからチャット履歴を閲覧されるリスク
- ツールの脆弱性で第三者により入力プロンプトを取得されるリスク

法的リスクも伴う…？

- 不正競争防止法
- 個人情報保護法

4-0. 生成AIの業務活用

- 営業部
- カスタマーサービス部
- 法務部
- 経理・財務部

※世の中に出ているAIを活用したサービスをもとに検討

4-1. 生成AIの業務活用「営業部」

活用方法	機密情報	個人情報
顧客の特徴や行動傾向予測	受注情報や購買タイミング情報、成約条件	顧客企業名や氏名、メールアドレス、役職などの名刺に書かれてる情報
商談トーク作成	見積もり情報や顧客の課題、提案の譲歩ライン、**提案の勝ちパターンといった営業ノウハウ**	社員名や顧客氏名、メールアドレス、所属部署
提案資料やメール作成	見積もり情報や顧客の課題、提案の譲歩ライン、提案の勝ちパターンといった営業ノウハウ	社員名や社員番号、顧客氏名、メールアドレス、電話番号、役職名、所属部署
顧客会議の議事録作成	**公開資料に残さないような「ここだけの話、正直なところ」**や顧客の課題、提案ノウハウ	社員名や顧客氏名、役職名、所属部署

4-2. 生成AIの業務活用「カスタマーサービス部」

活用方法	機密情報	個人情報
顧客のクレーム分析	**不具合情報**、対応時間や解決率などのデータ、サポート体制	顧客の氏名・住所・電話番号・メールアドレス、生年月日、購入履歴、**感情レベル**
業務FAQ作成	対応マニュアル、エスカレーション基準などの内部情報	ー
自動通話・チャットボット	問い合わせ内容	顧客の氏名、購入履歴、感情レベル、**録音音声**
問い合わせ内容の要約・翻訳	問い合わせ内容	顧客の氏名・メールアドレス、購入履歴

4-3. 生成AIの業務活用「法務部」

活用方法	機密情報	個人情報
契約審査 （契約書レビュー）	**公開していない契約内容**（代金、SLA、責任分担等）、契約交渉内容、添付資料に含まれる技術情報・製品情報等	契約書の署名者の氏名、個人事業主の氏名・住所、メールに含まれる自社/取引先従業員の氏名・メールアドレス等（自社ナレッジとして過去のやり取りメールも参照する場合）
法改正対応による 社内規程の更新	社内規程自体	―
法務相談の回答案作成	相談内容に含まれる機密情報 （M&A、新規事業など）	社員や関係者の氏名・メールアドレス等、顧客対応関連なら当該顧客名、**労務相談なら社員の健康状態や懲戒処分**等
特許調査 （特許の新規性や侵害リスクの調査）	**出願前の発明内容**	―

4-4. 生成AIの業務活用「経理・財務部」

活用方法	機密情報	個人情報
請求書・領収書処理 ・仕訳候補の自動生成 ・記載ゆれ統一	取引条件（単価・割引・支払条件）や仕入価格	個人事業主の氏名、住所、電話番号、メールアドレス
決算業務の効率化 ・前月差異が大きい科目の抽出と理由提示 ・異常仕訳の検知 ・締め処理のチェックリスト自動生成	売上・利益・原価・部門損益など**未公開数値**、**重要な経営判断に関わる分析資料**	ー
経営レポートの文章自動生成 ・PL/BS数値を要約 ・経営向けコメントを下書き ・予実差異の説明文を自動作成 ・会議資料のたたき台作成	**未発表**の業績／予算／M&Aや投資計画、主要顧客別・製品別の売上構成 経営会議資料	ー
給与・賞与処理 ・給与データの集計や支給控除の確認支援 ・年末調整データのチェック支援 ・締切/手続き等の問合せ対応のFAQ化	銀行口座番号、評価・報酬の個別情報	従業員の氏名、住所、電話番号、メールアドレスや、**健康、通院、扶養等の情報**など

4．生成AIの業務活用と不適切入力のリスク

RQ2

企業や組織において、どのように生成AIを業務活用でき、

どこに不適切な入力が発生するリスクがあるのか？

<u>活用方法と発生リスク</u>

- FAQやノウハウなどの社内ナレッジ作成時
- 顧客の特徴や経営データの分析時
- 各業務における問い合わせや提案文章の作成・要約時

<u>何が含まれる可能性がある？</u>

氏名やメールアドレスだけではなく、社内の未公開情報や社員の健康状態・懲戒処分、顧客の感情レベルなどの機微な情報

５．まとめ

**生成AIの業務活用と不適切入力のリスクについて、
2つの問いを立てて考察を行った。**

RQ1 **「生成AIへの不適切入力」は「内部不正の持ち出し」と比較し、どのような質的違いがあるか？その差に対する対策は？**

どちらも内部者による行為ではあるものの、不適切入力は非悪意で、「入力」という日常行為が起因で発生する。入力内容の定期的な確認や業務活用におけるリスク発生個所を把握することが重要である。

RQ2 **企業や組織で生成AIを業務活用する際に、どこに個人情報や機密情報の不適切な入力が発生するリスクがあるのか？**

FAQといった社内ナレッジの作成から顧客分析などを実施する際に、氏名やメールアドレスだけではなく、社内の売上情報や社員の健康状態・懲戒処分、顧客の感情レベルなどの情報をも入力し得るリスクがある。

ご清聴ありがとうございました

参考文献

[１. 研究テーマ]

- Siladitya Ray. ”サムスン、ChatGPTの社内使用禁止　機密コードの流出受け”. Forbes. 2023-05-03. 溝口慈子（翻訳）. https://forbesjapan.com/articles/detail/62905,（参照2026-02-25）
- 横山 信弘. ”《若手の一言》で会議室が凍りつき商談即中止､顧客ゲキ切れ　「AIで御社の課題を整理しました！」｢分かりやすい資料を作りたかった･･･」”. 東洋経済ONLINE. 2026-02-25 (再配信). https://toyokeizai.net/articles/-/918886,（参照2026-02-25）

[２. 内部不正による持ち出しと生成AIへの不適切入力]

- 株式会社リクルート. “当社元従業員による情報の持ち出しに関するご報告とお詫び”. 2025-08-01. https://www.recruit.co.jp/newsroom/pressrelease/2025/0801_143146.html,（参照2026-02-25）
- GIGAZINE編集部. “SamsungのエンジニアがChatGPTに社外秘のソースコードを貼り付けるセキュリティ事案が発生”. 2023-04-10. https://gigazine.net/news/20230410-samsung-chatgpt-security-leak/ ,（参照2026-02-25）
- IPA. “企業における営業秘密管理に関する実態調査2024」報告書概要”. 2025-08. https://www.ipa.go.jp/security/reports/economics/ts-kanri/j5u9nn0000004yjn-att/TradeSecret_summary_2024_r1.pdf,（参照2026-02-25）
- IPA. “組織における内部不正防止ガイドライン”. 2025-05-19（最終更新日）. https://www.ipa.go.jp/security/guide/insider.html,（参照2026-02-25）
- デジタル庁. “ChatGPT 等の生成AIの業務利用に関する申合せ（第2.1版）”. 2025-03-25. https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/debd5eca-6832-406e-a530-4e98ec032133/c60c5872/20250325_meeting_executive_agreement_07.pdf,（参照2026-02-25）
- CYBERSECURITY&INFRASTRUCTURE SECURITY AGENCY. ”Insider Threat Mitigation”. https://www.cisa.gov/topics/physical-security/insider-threat-mitigation,（参照2026-02-26）
- AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION. “SECURITY RECOMMENDATIONS FOR A GENERATIVE AI SYSTEM”. 2024-04-29 https://messervices.cyber.gouv.fr/documents-guides/security_recommandations_for_a_generative_ai_system.pdf,（参照2026-02-26）

[３．総務省・経済産業省『AI事業者ガイドライン』]

- 経済産業. “AI事業者ガイドライン”. 2025-04-04（最終更新日）.https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/20240419_report.html, （参照2026-02-25）

[４．生成AIの業務活用と不適切入力のリスク]

- 日本通信ネットワーク株式会社. “生成AIにより情報が漏洩した5つの事例｜原因や対策を詳しく解説”. 2025-07-04. https://www.c-ntn.co.jp/knowledge/info_leakage_ai/, （参照2026-02-25）
- 星野 和大. “生成AIの営業秘密漏洩リスクと企業の対策完全ガイド”. 株式会社feer. 2025-09-27. https://www.feer-design.com/magazine/sales/36, （参照2026-02-25）

- Salesforce Japan. “営業におけるAIの活用方法7選｜メリットや成功事例、注意点を紹介”. 2025-08-08. https://www.salesforce.com/jp/blog/jp-sales-ai/, （参照2026-02-25）
- パーソルビジネスプロセスデザイン. “パーソルP&T、Umee Technologiesと営業商談データを自動でAI解析し、 商談の“勝ち筋”を浸透・定着させる“イネーブルメントサイクル”を共同開発 『セールスイネーブルメントコンサルティングサービス』を提供開始”. 2024-06-04. https://www.persol-bd.co.jp/news/ppt/20240604/, （参照2026-02-25）
- DXコラム編集部. “営業にAIを活用するメリットとデメリット｜AIで解決できる営業課題を解説”. EXAWIZARDS. 2025-08-04（最終更新日）. https://exawizards.com/column/article/ai/sales/, （参照2026-02-25）
- PERSOL. “営業におけるAI活用例10選｜実際の活用シーンと合わせて解説”. 2025-05-30（最終更新日）. https://www.persol-group.co.jp/service/business/article/13120/, （参照2026-02-25）

[４．生成AIの業務活用と不適切入力のリスク]

- MNTSQ株式会社. “MNTSQ AI契約レビュー”. https://lp.mntsq.co.jp/aicontract-review, （参照2026-02-25）
- 株式会社KiteRa. “社内規程管理クラウド「KiteRa」、AIが法改正による規程改定案を提案する機能と参照元の条番号が変更された際、自動で参照先の条番号も変更される機能を新たに提供開始”. PRTIMES. 2023-07-10. https://prtimes.jp/main/html/rd/p/000000033.000045846.html, （参照2026-02-25）
- 安藤 俊幸, 特許調査への生成系AIの活用検討, 情報の科学と技術, 2024, 74 巻, Special_Issue 号, p. 2024-025, https://doi.org/10.18919/jkg.2024-025 (2024).

- 株式会社ニューラルオプト. “経理における生成AIの活用事例12選！決算・請求書処理・精算を効率化”2025-12-11（最終更新日）, https://neural-opt.com/accounting-gai-cases, （参照2026-02-25）
- 木内 翔大. “経理業務のAI導入事例7選！メリットや注意点も紹介”. AI経営総合研究所. 2025-12-12（最終更新日）. https://ai-keiei.shift-ai.co.jp/ai-accounting-example, （参照2026-02-25）
- NTT docomo. “生成AIで発生した情報漏洩の事例とは？さまざまなリスクと対策も紹介”. 2025-03-14（最終更新日）. https://anshin-security.docomo.ne.jp/security_news/privacy/column010.html, （参照2026-02-25）

- Cyber Security.com. “サポート詐欺被害で顧客情報等漏えい懸念｜住友林業クレスト株式会社”. 2025-04-17（最終更新日）. https://cybersecurity-jp.com/news/109505, （参照2026-02-25）
- 盛岡 麗. “Oktaで大量の顧客情報漏洩、カスタマーサポート管理システムへの不正アクセス”. 日経クロステック. 2023-11-30. https://xtech.nikkei.com/atcl/nxt/news/18/16368/, （参照2026-02-25）
- 三村. “アディダス、委託先へのサイバー攻撃で個人情報漏洩を公表”. セキュリティ対策ラボ. 2025-05-28（最終更新日）. https://rocket-boys.co.jp/security-measures-lab/adidas-reports-data-breach-via-customer-support-vendor-attack/, （参照2026-02-25）