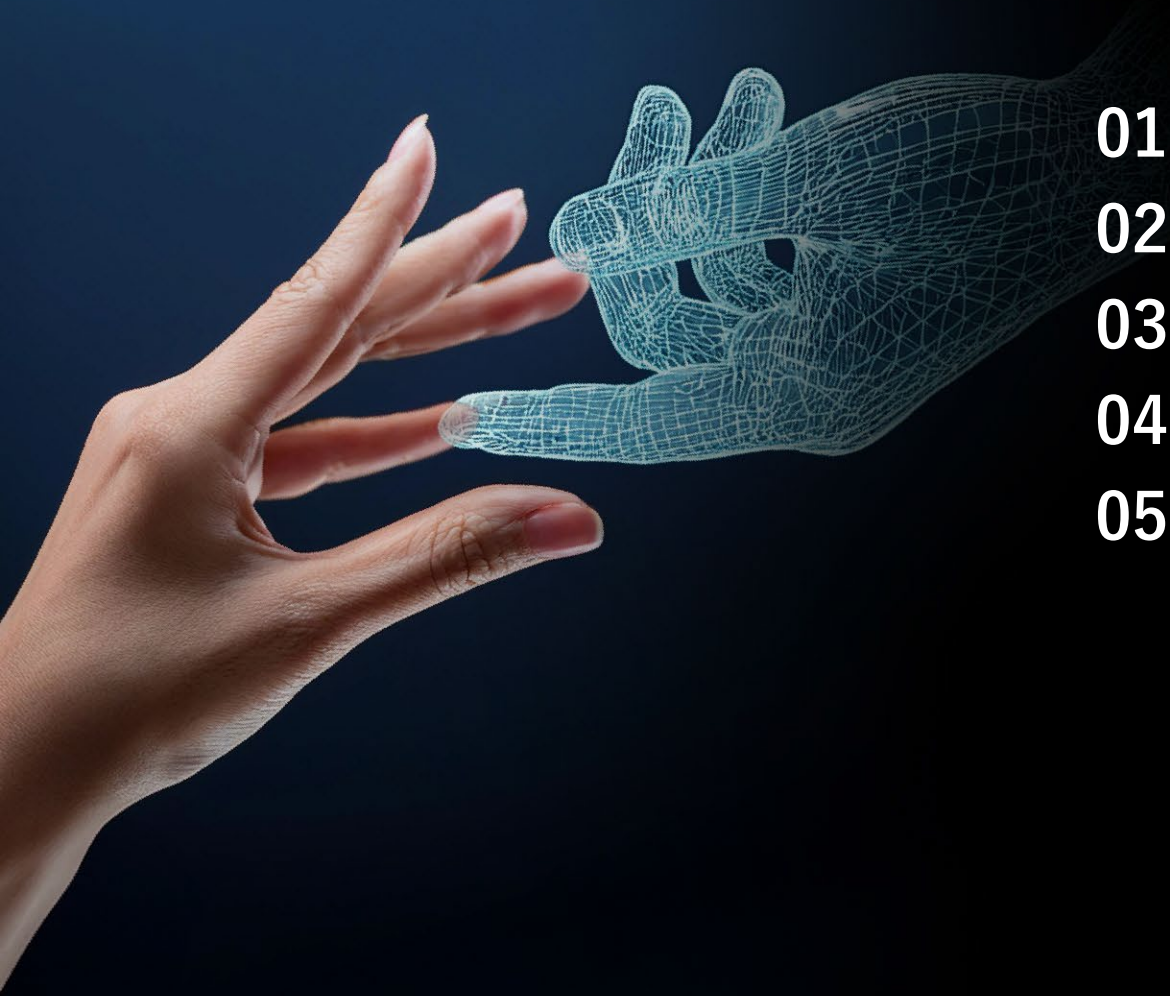
CAUAシンポジウム2025

IT企業における生成AI利活用ガイドライン

2025/11

伊藤忠テクノソリューションズ株式会社
ITセキュリティ統括部

目次



01　背景と世の中の動向

世の中の動向

- 生成AIは本格導入期へ
- 規制と標準が急速に整備
- リスク管理が競争力の鍵

AI に係る動向

2023年4月28日	CTC：生成系AIガイドライン (ChatGPT編）リリース
2023年12月	ISO/IEC 42001:2023 AIマネジメントシステムの発行
2024年4月	総務省及び経済産業省による「AI事業者ガイドライン（第1.0版）」の公表
2024年5月	EUで「Artificial Intelligence Act（欧州AI法）」が成立
2024年8月	内閣府によるAI制度研究会の開催、法整備に向けた有識者会議
2024年11月27日	CTC： 生成系AIガイドライン Version2.0リリース
2025年2月18日	経済産業省による「AI事業者ガイドライン実践のための契約チェックリスト」公表
2025年5月27日	デジタル庁が行政の進化と革新のための生成AIの調達・利活用に係るガイドライン公表
2025年 5月28日	「人工知能関連技術の研究開発及び活用の推進に関する法律（AI活用推進法）」成立
2025年 7月14日	CTC:　生成系AI社内利用ガイドライン Version3.0リリース
2025年9月1日	AI活用推進法の全面施行 / 内閣に「人工知能戦略本部（AI戦略本部）」が正式に設置され、「AI基本計画」の策定を開始

2　国の指針と国際標準

国内指針：AI事業者ガイドラインと契約チェックリスト

経済産業省・総務省の指針と実務対応

AI事業者ガイドライン

対象：開発・提供・利用者AI開発者、提供者、利用者の三者を対象としたガイドライン

人間中心と信頼の確保
AIシステムは人間の幸福と権利を尊重する原則

プライバシーと安全性
個人情報保護と堅牢なセキュリティ対策

透明性と説明可能性
AIの判断根拠を適切に説明できる能力

契約チェックリスト

再学習の可否を契約明記入力データが学習に利用されるかの確認と合意

データ所在と越境移転管理保存場所・国外移転の確認と法規制対応

責任範囲・保証・免責AI出力の責任所在とトラブル時の対応

権利帰属とIPの整理生成物の著作権所在と二次利用条件の明確化

企業リスクと対応策

課題認識とガイドライン策定の軸

⚠ 企業が直面する三つのリスク

情報漏えいリスク
機密情報・個人情報の入力再学習による第三者への拡散クロスボーダー移転の法的課題

著作権侵害リスク
学習データの権利処理問題生成物による既存著作物の模倣訴訟事例の増加

品質・幻覚リスクHallucination（幻覚）
不正確な情報による判断ミスレピュテーションへの悪影響

🛡 三つの観点からの対応策

情報セキュリティの観点
機密情報管理・再学習リスクへの対策再学習オプトアウト利用の推進クロスボーダー移転リスク評価

法令遵守の観点
著作権侵害・個人情報保護への対応学習データの権利処理確認生成物の2次利用権の確認

ガバナンスの観点
マネジメントシステム・人的確認・品質保証出力内容の検証プロセス確立利用ログの記録と追跡可能性

03　CTCグループにおける生成AIガイドライン

CTCグループにおける生成AIガイドラインの現在の位置づけ

生成AIガイドラインの特徴

- ISMS基盤の上に整備
- 利活用促進志向のガイドライン
- 国指針・ISOと整合
- 継続改訂で実効性確保

基本方針と対象範囲

基本方針	生成AIの利活用の推進
ガイドライン策定の基本的アプローチ	ISMSに整合： 既存規程に則り、新たな制限を付加せず 対象範囲： 国内CTCグループ役職員の業務利用のみ 入出力の管理： 入力データと出力結果を区分して管理 再学習確認： AIサービスが再学習するか事前確認を徹底 判断基準： 現場で即断できるシンプルで明確なルール

法令遵守

法令遵守：課題と対応

著作権と個人情報の観点から

【主な課題】

著作物の模倣・流用リスク

個人情報の第三者提供懸念

海外サーバー保存の適法性

【対応策】

模倣目的の入力を禁止（他目的は許可）

再学習しないAIのみ個人情報入力を許可

海外保存はイントラでの確認フローを簡素化

生成系AI社内利用ガイドライン　Ver3.0　概要

ガイドライン概要

法令や契約を遵守しつつ利活用の促進

模倣・流用目的以外で第三者の著作物を入力等することは可能

入力等された情報が再学習に利用されないことを前提に個人情報、機密情報の入力等が可能

生成物はそのまま利用せず、必ず人の目でチェックし、必要に応じて修正（削除やマスキング）し、利用に関する同意の取得等の適切な対応の実施

生成物利用時は、内容の不正確や、著作権上の問題、個人情報、機密情報が含まれるといったリスクがあることを留意

生成AI　社内利用

社内イントラに専用ページ

社内での利活用を促進するため整備

再学習しない生成AIの解説

海外サーバへの個人データ保存についての注意事項

安全管理措置が確認された生成AI製品

原則利用禁止となる生成AI製品とその理由

利用検討している生成AIの安全性の確認ポイント

生成物チェックと支援体制

生成物チェックプロセス

1. 生成AIによる出力
   生成AIが作成したコンテンツ
2. 人の目で確認
   そのまま利用せず必ずチェック
3. 機密・個情マスク
   不適切な情報を削除・修正
4. 著作権確認
   第三者の権利を侵害していないか
5. 社外利用時の同意確認
   必要に応じて関係者の承認

支援体制と運用設計

- FAQ整備
  社内イントラに最新情報を掲載
  適宜アップデート
- 判断基準
  現場担当者が判断しやすいよう社内イントラに掲載
- 相談窓口の一元化
  迷った場合の相談先を明確化
- 安心して利用できる生成AIをリスト化
  安全性が確認されている生成AIサービスを社内イントラに掲載

バージョン管理と主要変更点

ガイドラインの変遷

2023/4/27　Version 1.0

OpenAI ChatGPTに特化

- 機密情報・個人情報の入力禁止

2024/11/27 Version 2.0

対象を全生成AIに拡大　ISMS基盤上に整備

- 機密情報を自社/他社で個別判断
- 個人情報の入力条件と海外サーバー確認フロー整備

2025/07/14 Version 3.0

機密情報の入力条件大幅緩和

- 個人情報の確認プロセス簡素化
- 契約チェックリストとAI事業者GLに準拠

主要変更点と判断軸

項目	Version 2.0	Version 3.0
機密情報	自社/他社の機密情報で個別判断	再学習しないことを前提に入力可能
個人情報	海外（サーバー）保存時の事前問合せ必須	社内イントラでの確認フローへ簡素化

改訂の判断軸

利便性とセキュリティのバランス：現場での判断負荷を軽減

既存ISMSとの整合性：ISMSルールを遵守しつつ効率化

国の指針・標準との整合：AI事業者ガイドラインの更新に対応

ISO27001とISO42001の親和性

	ISO/IEC 27001（ISMS）	ISO/IEC 42001（AIMS）
構造	10章構成のマネジメントシステム規格（MSS）	同じく10章構成のMSS　意図的に整合性を確保
対象	情報資産全般のセキュリティ	AIシステムの管理　（開発・提供・利用）
リスク管理	情報セキュリティリスク　（機密性・完全性・可用性）	AIリスク（倫理・安全性・信頼性・品質）
セキュリティ連携	組織的・物理的・技術的管理策 アクセス制御・暗号化	AIデータの保護に応用可能 学習データ・モデルパラメータの保護
個人情報保護	個人情報保護法対応（PMS連携）	AIデータバイアス防止・プライバシー強化型AI設計
データガバナンス	情報分類・ライフサイクル管理	学習・推論データの品質管理・AIモデル追跡・監査証跡
管理策	93管理策（附属書A）	38管理策（附属書A）　AI特化の対策集
技術的管理策	脆弱性管理・インシデント対応 通信セキュリティ	AIモデル堅牢性・自動攻撃検知　説明可能性確保
親和性	既存インフラの活用	高い構造的整合性 ISMSを基盤として拡張可能 文書体系やプロセスの流用可能

04　今後の動向

国際・国内法規制の段階適用

EU AI法の段階適用

EU域内で直接適用される規則(Regulation)。域外企業への越境適用あり。違反時は最大グローバル売上高の7%の制裁金。

2025年2月2日

許容できないリスクAI禁止

社会的スコアリングシステムや脆弱な人々を搾取する操作的技術など、「許容できないリスク」に分類されるAIシステムの使用が全面的に禁止

EU市場向けAIサービスの禁止カテゴリ審査必須

2025年8月2日

汎用AI（GPAI）モデル規則適用

汎用AIモデルに関する規則が適用開始。基盤モデル提供者の透明性義務、情報開示、リスク評価が義務化

主要LLM・画像生成AI等への規制適用開始

2026年8月2日

ハイリスクAIシステム規則施行

大部分の規定が施行され、附属書IIIに記載されたハイリスクAIシステムに関する義務や、透明性に関する規則が適用開始

適合性評価・監視体制の義務化

2027年8月2日

既存規制製品組込みAI適用

医療機器や自動車安全システムなど、既存の規制製品に組み込まれたハイリスクAIシステムに関する規則が全面適用

日本企業の越境取引への規制影響が全面化

日本AI活用推進法の施行

「人工知能関連技術の研究開発及び活用の推進に関する法律」。促進型・基本法的性格の法律。主務大臣：内閣総理大臣。

2025年5月28日

法律成立

参議院本会議で可決成立（全会一致）。国会審議を経て法案成立。

国内初のAI専門法として位置づけ確立

2025年9月1日

全面施行・組織設立

内閣に「人工知能戦略本部（AI戦略本部）」設置。

国家レベルのAI推進体制確立

2025年9月中旬

基本計画骨子の公表

内閣府が「人工知能基本計画（骨子・たたき台）」を公表。

国のAI戦略の方向性が具体化

2025年10月3日

AI法施行フォロー

内閣府（CAO）が「AI法全面施行」等のフォロー（広報）を公表。企業向け説明会や相談窓口の設置。

企業の法令対応支援が本格化

2025年10月～

「AI基本計画」策定開始

5年間の推進計画・予算措置。業界別ガイドライン整備。人材育成・安全確保・国際連携の推進。

産業界の自主規制と国の支援策の連動

国際標準と実務ガイドライン・AI安全性評価の標準化

AIガバナンスの枠組み整備

国際標準と実務ガイドライン

ISO/IEC 42001認証制度

- 2025年7月：日本での認証開始
- 2025年8月20日：JIS Q 42001:2025発行
- 国際的な信頼性指標としての地位確立
- 企業間取引の要件化の動き
  ※

AI事業者ガイドラインの進化

- 2025年3月：第1.1版に更新
- 生成AIモデルに関する留意事項
- 追加契約条項例の拡充
- ガイドライン継続改訂と実務への反映

契約チェックリストの普及

- 生成AI活用の契約実務標準化
- 再学習有無・データ保存場所の明確化
- 責任分界点の標準的条項の普及

国内AI安全性評価の標準化

IPAのAIセーフティ・インスティテュート(AISI)の取り組み

2025年9月16日：AIセーフティ評価ツールをOSS公開 AIシステム開発者・提供者向けの評価環境提供

有害情報制御　偽誤情報防止　公平性　ハイリスク対処　プライバシー　セキュリティ　説明可能性　ロバスト性　データ品質　検証可能性

IT企業としてしての今後の方向性

生成AI利活用推進にむけて

利用実態の可視化：ログ分析・アンケート調査による活用状況モニタリングと効果測定

ISO/IEC 42001認証検討：既存ISMS基盤を活用したAIマネジメントシステムの導入

グローバル展開：海外拠点への展開と各国規制への対応

業界標準への貢献：ガイドライン策定ノウハウの共有と標準化活動

顧客支援：ガイドライン策定支援、AI導入コンサルティング、リスクアセスメント支援、運用支援サービス

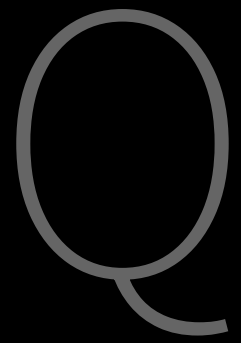
04　まとめ

まとめ

ガイドライン策定の4つの鍵

- ISMS整合で実効性確保
- 国指針・ISOと整合
- 使いやすさ重視の設計
- 継続改善のPDCA

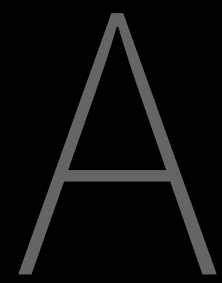
質疑応答

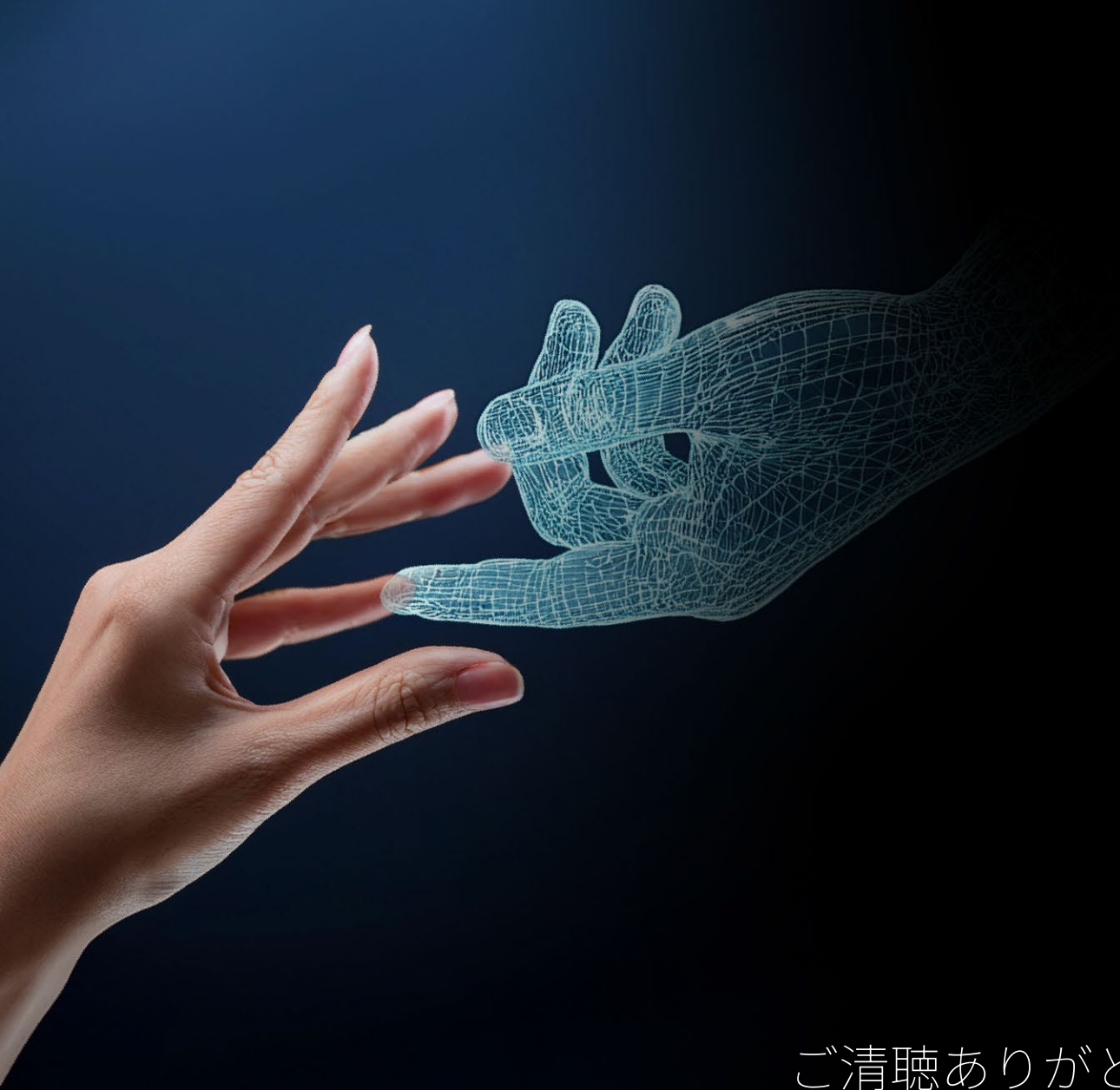


質疑応答

ご質問をお受けします

連絡先：takeshi.murai@ctc-g.co.jp





CTC

Challenging Tomorrow's Changes

ご清聴ありがとうございました