

報道関係者各位

2024年3月5日

EGセキュアソリューションズ株式会社

エムオーテックス株式会社

## Webセキュリティ専門家 徳丸 浩 監修 『AIサービス利用ガイドライン』をリリース ～ AIサービス業務利用時の注意点・確認事項を分かりやすく解説～

EGセキュアソリューションズ株式会社 (<https://www.eg-secure.co.jp/> 東京都港区 代表取締役：高谷 康久 以下「EGセキュアソリューションズ」と、エムオーテックス株式会社 (<https://www.motex.co.jp/> 大阪市淀川区、代表取締役社長：宮崎 吉朗、以下「MOTEX」) は、Webセキュリティ専門家でEGセキュアソリューションズ取締役CTOの徳丸 浩が監修した、AIサービス業務利用時の注意点・確認事項をまとめた『AIサービス利用ガイドライン』(ダウンロード可能なPDFデータ/無償)をMOTEXが提供開始したことを発表します。

◎ダウンロードはこちら(無料) ※MOTEXのフォームに遷移します

[https://www.lanscope.jp/endpoint-manager/form\\_documents/AI\\_service\\_guideline\\_2402\\_EM063/](https://www.lanscope.jp/endpoint-manager/form_documents/AI_service_guideline_2402_EM063/)



昨年2023年は「生成AI元年」とも称され、OpenAI社が開発したChatGPTをはじめとする生成AI技術を活用したAIサービスが急速に普及しました。これにより、個人だけでなく企業・組織においても、業務効率化を目的とした活用やビジネスへの取り込みなど、AIによるデジタルトランスフォーメーション(DX)が加速しています。

しかし、その一方で、ビジネスシーンにおけるAIサービス利用には、企業・組織におけるセキュリティ上の課題も存在します。例えば、従業員が業務に関連する情報収集や文章作成、翻訳、あるいはプログラミングといったシーンで、AIサービスへの質問・投稿内容に個人情報や機密情報が含まれていると、その情報がサービス提供事業者側に収集されてしまう可能性があります。また、生成AIの回答は事実ではない内容が含まれる可能性があります。こういった生成AIならではの注意点を知らずに利用することで問題を起こしてしまう可能性もあり、AIサービスの仕組みならではの情報漏洩リスクが指摘されている状況です。

企業・組織におけるセキュリティ対策では、従業員に対しセキュリティ方針を示し、ガイドラインを周知して遵守することが基本的かつ重要なポイントです。しかし、多くの企業・組織における実態としては、新たな技術であり、進歩が速い生成 AI に対応したガイドラインを作成することへの敷居が高く、思うように生成 AI の活用を進められていなかったり、従業員が申告せずに利用するなどのいわゆる「シャドーIT」となってしまったりといった課題があります。

そこで今回、セキュリティ企業として企業・組織の IT 環境の安心・安全に携わる EG セキュアソリューションズおよび MOTEX では、Web セキュリティ専門家 徳丸 浩（イー・ガーディアングループ CISO 兼 EG セキュアソリューションズ 取締役 CTO）監修のもと『AI サービス利用ガイドライン』を作成しました。AI サービスを業務で利用する際の注意点・確認事項を、生成 AI ならではの注意点や事例も交え、専門的な視点で分かりやすくまとめており、自社・自組織のガイドライン作成の目安としていただくことができます。

下記 URL より、無償で PDF データをダウンロードいただけますので、AI サービスの業務利用を検討されている方、社内の指針・ルールの方策や従業員への注意喚起にお悩みのセキュリティ担当の方のお役に立てば幸いです。

◎ [ダウンロードはこちら（無料）](#) ※MOTEX のフォームに遷移します

[https://www.lanscope.jp/endpoint-manager/form\\_documents/AI\\_service\\_guideline\\_2402\\_EM063/](https://www.lanscope.jp/endpoint-manager/form_documents/AI_service_guideline_2402_EM063/)

## ■ 『AI サービス利用ガイドライン』の概要

- ・ガイドラインの目的
- ・用語の定義
- ・AI サービス利用の前提
- ・AI サービスへの入力を禁止する項目
- ・AI サービスの応答内容を利用する際の注意点
- ・活用場面から見る AI サービス利用の法的リスク
- ・オプトアウト機能について
- ・補足：報道されている AI サービスを使った事件
- ・補足：よりよく AI サービスを使うために

◎ [ダウンロードはこちら（無料）](#) ※MOTEX のフォームに遷移します

[https://www.lanscope.jp/endpoint-manager/form\\_documents/AI\\_service\\_guideline\\_2402\\_EM063/](https://www.lanscope.jp/endpoint-manager/form_documents/AI_service_guideline_2402_EM063/)

## ■ イー・ガーディアングループ CISO 兼 EG セキュアソリューションズ 取締役 CTO 徳丸 浩 コメント

イー・ガーディアングループは、経営理念「We Guard All」に基づき、総合ネットセキュリティ企業として一貫通貫のソリューションを提供しております。

生成系 AI を始めとする AI サービスは急速な普及を見せ、活用事例も多く報道されているところではありますが、正しい使い方に関する議論は始まったばかりです。生成系 AI は便利で、働く人の生産性向上に大きく寄与することは疑いありませんが、一方で、セキュリティや権利侵害、コンプライアンス、法務的な問題など、利用の上での課題も多く存在します。

本ガイドラインをベースとして利用企業各位の事情に合わせたガイドラインを策定していただくことで、AI サービスを安心して活用いただける環境づくりに寄与できれば幸いです。

**<経歴>**

イー・ガーディアングループ CISO 兼 EG セキュアソリューションズ株式会社 取締役 CTO。

Web アプリケーションセキュリティの第一人者。脆弱性診断やコンサルティング業務のかたわら、ブログや勉強会などを通じてセキュリティの啓発活動を行う。著書『体系的に学ぶ 安全な Web アプリケーションの作り方 第2版』は「徳丸本」と呼ばれ、広く Web 従事者に支持されている。

**■ MOTEX 取締役 CISO 中本 琢也 コメント**

MOTEX は「Secure Productivity (安全と生産性)」というミッションのもと、「LANSCOPE」ブランドのプロダクト・サービスの提供を通じて、お客様が安心してエンドポイントやネットワーク、IT サービスをご利用いただけるビジネス環境の構築をご支援しております。

昨今大きな注目を集めている ChatGPT などの生成 AI は、従来からの IT サービス利用時に注意すべきポイントだけでなく、生成 AI ならではの注意ポイントが多数存在しています。

弊社では、昨年より生成 AI がビジネスやサイバーセキュリティにどのような影響をもたらすのかを考えるセミナーや、生成 AI の業務利用を前提とした製品機能のリリース(\*)などを行ってまいりましたが、その中で、「ガイドラインを策定する必要に迫られているが、どのように作成すればよいのか分からない」「セキュリティ上のリスクを払拭できず、一律で生成 AI の利用を禁止してしまっている」「不安を抱えたまま生成 AI を利用している」といったお客様からのお声を伺いました。

本ガイドラインは、セキュリティに専門的知見をお持ちの徳丸様にも監修いただき、生成 AI ならではのポイントもカバーした内容となっております。皆様の組織のセキュリティ対策や生成 AI 活用促進の一助となれば幸いです。

\*関連情報 | MOTEX が提供する統合エンドポイント管理「LANSCOPE エンドポイントマネージャー」、ChatGPT への書き込みログ取得機能を実装 (2023 年 6 月)

<https://www.motex.co.jp/news/release/2023/release230629/>

**【MOTEX について】**

MOTEX は「Secure Productivity」をミッションに掲げ、プロダクト・サービスの提供を通じて、お客様が抱えるサイバーセキュリティの課題解決を支援します。安全と生産性の両方を実現し、お客様がエンドポイントやネットワーク、IT サービスを安心してご利用いただけるよう、これまで培ってきた技術と豊富な知見で、世界水準のプロダクト・サービスをご提供します。

**■ エムオーテックス株式会社 (MOTEX) 会社概要**

代表者 : 代表取締役社長 宮崎 吉朗

所在地 : 大阪市淀川区西中島 5-12-12 エムオーテックス新大阪ビル

設立 : 1990 年 7 月

資本金 : 2,000 万円

業務内容 : サイバーセキュリティに関するプロダクト開発・サービス事業

株主 : 京セラコミュニケーションシステム株式会社 (資本比率: 100%)

URL : <https://www.motex.co.jp/>

**【イー・ガーディアングループについて】**

1998年設立。2016年に東証一部上場。2022年に東証プライム市場へ移行。イー・ガーディアンはネットパトロール、カスタマーサポート、デバッグ、脆弱性診断などネットセキュリティに関わるサービスを一通貫で提供する総合ネットセキュリティ企業です。センターは、提携先を含めてグループで国内8都市海外3都市19拠点の業界最大級の体制を誇ります。昨今はFintech・IoT業界への参入やRPA開発による働き方改革への寄与など、時代を捉えるサービス開発に従事し、インターネットの安心・安全を守っております。

**■EGセキュアソリューションズ 会社概要**

代表者 : 代表取締役 高谷 康久

所在地 : 東京都港区虎ノ門 1-2-8 虎ノ門琴平タワー8F

設立 : 2008年4月

資本金 : 1,000万円 (2023年3月末日現在)

業務内容 : 1. 情報セキュリティ、情報システムに関する監査、コンサルティング  
2. 情報セキュリティに関する調査、研究、執筆  
3. 情報セキュリティ関連の教育及びコンテンツ制作  
4. セキュリティ製品の開発、販売、サポート

URL : <https://www.eg-secure.co.jp/>