

中小企業のセキュリティ対策

AI利用時のリスク啓発

(独立行政法人情報処理推進機構・江島将和)

最低限の対策示す「豆知識」作成

近年、生成AIをはじめとする高度なAI技術の実用化が急速に進む一方で、AIの悪用や脆弱性（ぜいじゃくせい）を狙った攻撃など、セキュリティ上の課題が顕在化しており、独立行政法人情報処理推進機構（IPA）が2026年1月に公開した「情報セキュリティ10大脅威2026」では、「組織」向け脅威の第3位に「AIの利用をめぐるサイバーリスク」がランクインしている。AIの利活用が進む中、AIの利用者と開発者の双方に向けた一層のセキュリティ対策の強化とその普及・啓発が求められている。

こうした中、IPAおよびAIセーフティ・インスティテュート（AISI）は、安心・安全なAI利用の推進を目的に、25年より有識者や業界団体と共にAIセキュリティに関する検討を重ねてきた。その活動の成果として、AIセキュリティ啓発を目的とした「AI利用者のためのセキュリティ豆知識」を公表した。

AI利用者のためのセキュリティ豆知識は、AIやセキュリティの基本を理解したい利用者を対象に、AIを利用する際に最低限実施すべきセキュリティ対策を分かりやすくまとめたものである。

AIセキュリティ対策として、次の五つの対策を挙げている。

実施すべき 五つの対策

- ①クラウドAIに営業秘密は教えない
- ②AIブラウザは社内用と社外用を分ける

- ③RAG（Retrieval Augmented Generation＝検索拡張生成）使用時は「混ぜるな危険」にご用心
- ④外見では詐欺師を見破れないと心得る
- ⑤AI仕込みのサイバー攻撃も撃退法は従来通り

③のRAGは、生成AIが検索で知識を補う仕組みのこと。RAGを使うことで自社の社内情報に即した回答を生成AIから得られるようになる一方で、どのデータをRAGの検索対象にするかどうかはセキュリティも考慮して決める必要がある。

AI利用者のためのセキュリティ豆知識は、社内研修などでそのまま利用できるプレゼンテーションスライド形式で提供しており、今後のAI利用ケースの拡大に合わせて継続的に更新していく予定となっている。

開発者向け情報「短信」も公開

また、IPAではAIシステム開発者やセキュリティ担当者を対象に、AIセキュリティに関する最新のトレンドや事例を紹介した「AIセキュリティ短信」を公開した。日々発信される膨大な情報をAIセキュリティの観点で整理しており、これまでは有識者や業界団体向けに不定期で配信してきたが、より多くのAI・セキュリティ担当者に知っていただきたいとの業界団体からのご意見を受けて、最新号（26年3月号）およびこれまで作成した3号分を公開した。

AIやセキュリティそれぞれの専門家はいても両分野に精通した人材はまだ多くないという現状を鑑み、啓発への一助となることを期待している。



AIを活用することで業務の効率化が図られるとともに、生産性の向上を期待することができる。一方で、セキュリティに留意する必要がある。IPAとAISIでは、今後もAIの利活用とAIセキュリティに関する情報を発信していくので活用いただきたい。

(会議所ニュース5月21日号(日本商工会議所発行)より転載)

AI利用者のためのセキュリティ豆知識

公開版

1. クラウドAIに営業秘密は教えない

IPA

67%

の従業員が個人アカウントで生成AIツールを使用している

77%

の従業員が生成AIツールにデータを「貼り付け」している

32%

法人から個人利用のサービスに「貼り付け」されるデータの32%は生成AIツールが受皿

インターネット経由で利用できるクラウド型のチャットAIに営業秘密を話すとチャットAIの運営企業にその営業秘密が渡ってしまいます

チャットAIとユーザーとの実際のやりとりを将来のAI改良のための学習データとして運営企業が流用する場合があります

自社の営業秘密を学習したAIはその内容を他のユーザーに喋ってしまう可能性が理屈上あります

利用するチャットAIのサービス規約やチャットAIの利用時設定を確認することでユーザー入力を保存やAIの学習対象から除外できます

AIツールへの情報漏洩実態 (LayerX Security 社調査)

<https://www.layerx.co.jp/ai-security/>

2026/03

© 独立行政法人情報処理推進機構 2026

「IPAのAIセキュリティへの取り組み」
についてはこちらを参照

