

TRAINING

AI時代に学ぶサイバーセキュリティ

1日目 生成AIと情報セキュリティ

スタッフサービス・エンジニアリング様 派遣エンジニア向けオンラインセミナー

2026年11月17日（火） 全3回の1回目



本資料の二次転載禁止について

本資料は株式会社ギブリーが作成した研修教材であり、著作権法により保護されています。受講者ご本人の学習目的に限りご利用いただけます。無断での複製、改変、第三者への提供、社外への公開は禁止です。本資料に掲載した外部サービスとニュースの画面は、各社の権利に帰属します。

講師紹介



人的資本インテリジェンス部門講師
生成AIエバンジェリスト

安田 光喜

Mitsuki Yasuda

メッセージ

みなさんがこれから生成AIをパートナーに新しい時代を生き
ていけるように、3日間全力でサポートしていきます！なに
かご不明点などありましたら、講師陣になんでも気軽にご質
問ください。

#ClaudeCode #Codex #Cursor #Antigravity
#全国統一生成AI活用技能試験S1 #生成AIサポート #G検定

得意領域

- ・生成AIをはじめとした世界最先端トレンド
- ・生成AIを用いた新規事業の開発、運営、補助
- ・アプリケーション開発/自動化プログラム環境構築
- ・教育（大学講師、研修、スクール運営など）

実績

- ・生成AI研修
- ・大手企業、外資、教育機関(小中高大)での
ITトレンド講演
- ・自治体と連携した地域教育実績
- ・上場企業社員対象のリスキリング支援

公立はこだて未来大学 大学院（メディアデザイン領域）を卒業し、街づくり会社での複合商業ビルの立ち上げにおける情報インフラ整備やデザイン全般業務の責任として関与。その後デザイン事務所を立ち上げ、飲食店を中心としたデザイン業務や美術館展示のアートコンテンツ開発などを行う。また、地域ブランディングにも注力し、市主催の企画運営業務を行なった。2018年10月『小中学生向けのプログラミング教育』に注目し、函館市で初めての小中学生向けプログラミングスクール『D-SCHOOL北海道』を立ち上げて運営。その後北海道のドラッグストア『サッポロドラッグストアー』からスクールの買収を受け、教育を専門とするグループ会社『株式会社シーラクス』にて技術開発責任者として運営。スクール設計・運営、20以上の自治体連携（イベントや出張教室運営）、大人向けプログラミングスクールメンターなどさまざまな『次世代IT教育』に取り組む。

Dify公式資料の日本語翻訳や、SecondMeアンバサダーなど生成AI最新トレンドに注力。

全3回の進み方

全3回は「知る」「守る」「対応する」の3ステップ

1日目 知る

11月17日（火）
生成AIと情報セキュリティ。AIが攻撃と社内の使い方をどう変えたかを知ります

2日目 守る

11月25日（水）
世界のハッキング事例と個人での対処法。自分のアカウントと端末を点検します

3日目 対応する

11月27日（金）
会社としての対処法とこれからの考え方。事故の初動と報告文を作ります

各回だけの参加でも分かるように作っています。前の回の要点は、毎回の始めに振り返ります。

本日の流れ

前半は講義で後半はGeminiを使うハンズオン

枠	内容	形式	時間
S01	本日の到達点と進め方	講義	[10min]
S02	生成AIが変えた攻撃	講義	[25min]
S03	社内のAI利用に潜む穴	講義	[25min]
S04	ハンズオン 生成AIに入れてよい情報の仕分け	ハンズオン	[40min]
S05	ふりかえりと次回まで	講義	[10min]
閉会	質疑応答		[10min]

本日の到達点

本日の終わりにできるようになること

- 1 攻撃する側がAIで何を変えたかを、事例と数字で説明できる**
なりすましの電話、AIで作ったフィッシング、10代が作ったランサムウェア
- 2 社内のAI利用に潜む穴を、自分の職場に当てはめて挙げられる**
会社が把握していないAI利用と、AIエージェントの事故
- 3 業務の情報を3段階に仕分け、匿名化してからAIに渡せる**
ハンズオンで、仕分けシートと匿名化したメモを作ります

AI時代のセキュリティ

AIの広がりでセキュリティの**重要性が上がっている**

3 位

IPAの10大脅威 2026の組織編で、「AIの利用をめぐるサイバーリスク」が初めて選ばれた順位

4件に1 件

悪意ある侵害のうち、攻撃者がAIを使っていた割合（IBMの2026年版調査）

123 件

2026年上半期に警察庁が把握したランサムウェアの被害。半期で過去最多

出典 IPA「情報セキュリティ10大脅威 2026」、IBM Newsroom（2026年7月29日、Cost of a Data Breach Report 2026の発表）、警察庁「令和8年上半期におけるサイバー空間をめぐる脅威の情勢等について」

情報セキュリティ10大脅威 2026

組織編の3位にAIの利用をめぐるリスクが初めて入った

▲ 情報セキュリティ10大脅威 2026 [組織]

順位	「組織」向け脅威	初選出年	10大脅威での取り扱い (2016年以降)
1	ランサム攻撃による被害	2016年	11年連続11回目
2	サプライチェーンや委託先を狙った攻撃	2019年	8年連続8回目
3	AIの利用をめぐるサイバーリスク	2026年	初選出
4	システムの脆弱性を悪用した攻撃	2016年	6年連続9回目
5	機密情報を狙った標的型攻撃	2016年	11年連続11回目
6	地政学的リスクに起因するサイバー攻撃（情報戦を含む）	2025年	2年連続2回目
7	内部不正による情報漏えい等	2016年	11年連続11回目
8	リモートワーク等の環境や仕組みを狙った攻撃	2021年	6年連続6回目
9	DDoS攻撃（分散型サービス妨害攻撃）	2016年	2年連続7回目
10	ビジネスメール詐欺	2018年	9年連続9回目

- 1位はランサム攻撃による被害で、11年連続
- 2位はサプライチェーンや委託先を狙った攻撃
- 3位の「AIの利用をめぐるサイバーリスク」は初めての選出
- IPAは約250人の選考会の審議と投票で順位を決めています

出典 IPA「情報セキュリティ10大脅威 2026」

これから求められる人

セキュリティの知識はAIを使う**全員**に要る

AIを使って働く人

- 生成AIに渡す情報を、毎日自分で判断しています
- 入れてはいけない情報を入れると、攻撃がなくても情報が外に出ます
- おかしいと気づいたら止めて、相談するところまでが仕事に入ります

守りを専門に担う人

- 監視（SOC）、脆弱性診断、クラウドの設定点検、インシデント対応を担います
- DXとクラウドとAIの広がり、需要が高まっています
- 気づいてから対応するまでを、一連でこなせる人が求められています

セキュリティ人材の不足

不足しているスキルの首位はAI

約11万人

国内で不足しているとされる
サイバーセキュリティ人材
(ギブリーが紹介した推計)

41%

セキュリティの専門家が、自分
のチームに足りないと答えた
スキルの首位がAI (ISC2の
2025年調査)

24項目

ギブリーのスキル標準2026の
100項目のうち、AI時代の観点
を付けた項目

出典 ギブリー「サイバーセキュリティスキル標準 2026」、ISC2（2025年のサイバーセキュリティ人材調査）

S02

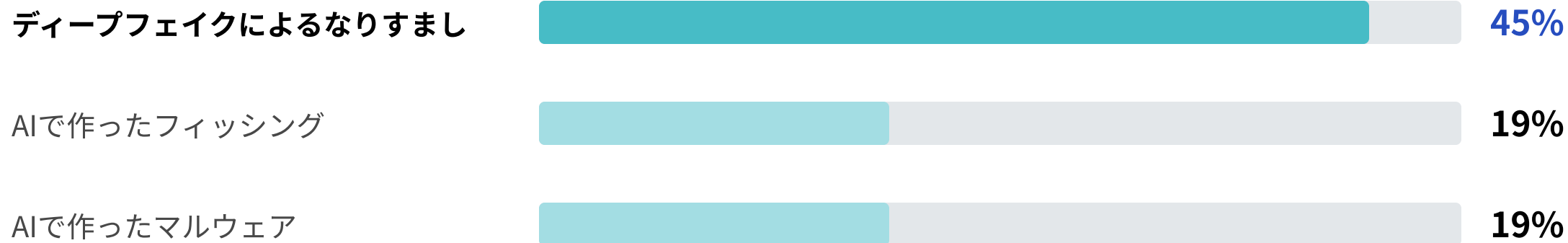
生成AIが変えた攻撃

攻撃する側は、AIを日常の道具として使い始めている

- AIを使った侵害の内訳
- 本物に見える声と映像
- 10代がAIで作った攻撃の道具
- AIエージェントが担う侵入の作業

AIを使った侵害の内訳

AIを使った侵害の45%はディープフェイクのなりすまし

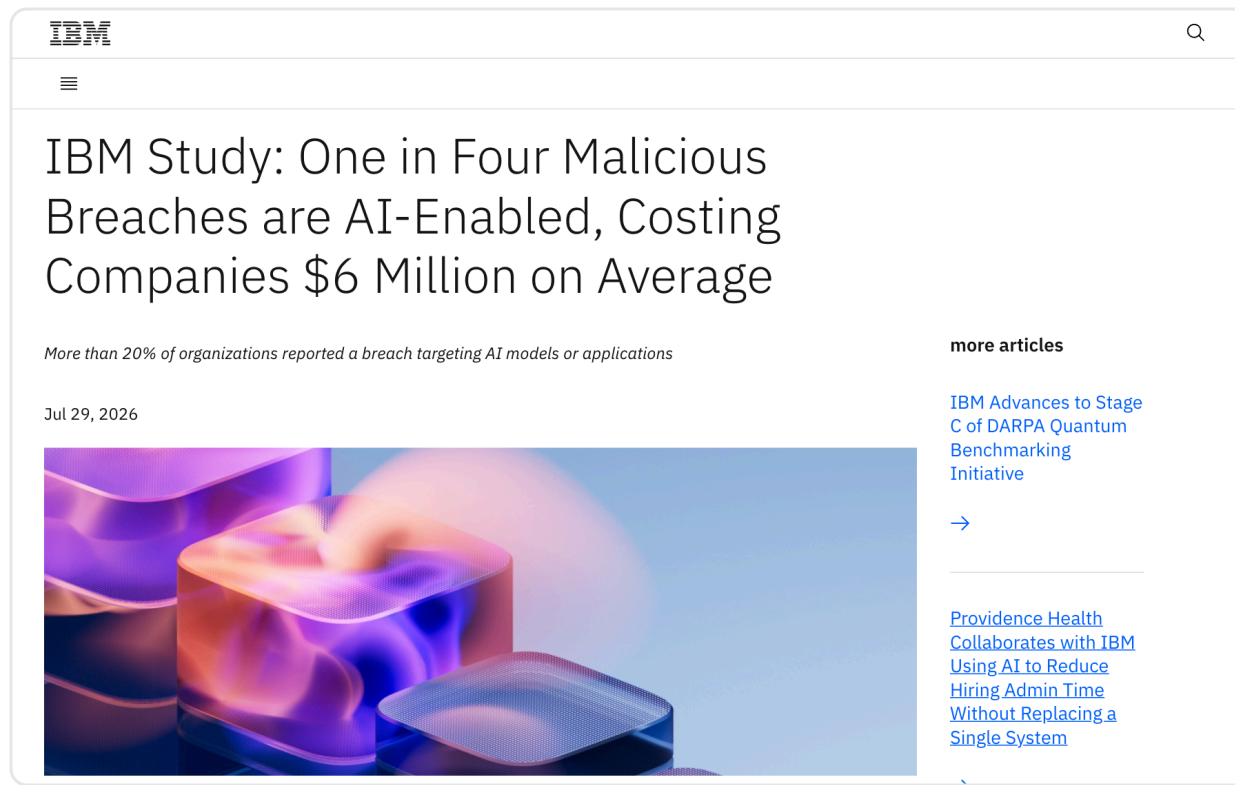


悪意ある侵害の4件に1件でAIが使われていました。上の割合は、そのAIを使った侵害の中での内訳です。

出典 Baker Donelson (IBMの2026年版調査の要点)

IBMの2026年版調査

AIを使った侵害は1件あたりの費用も高い



- AIを使った侵害は、前年より56%増えました
- AIを使った侵害の平均費用は約600万ドルです
- 世界の侵害の平均費用499万ドルより、約100万ドル高い額です

出典 IBM Newsroom (2026年7月29日、Cost of a Data Breach Report 2026の発表)

本物に見える声と映像

入口はメールから電話へ広がっている

数字で見る変化（M-Trends 2026）

- 2025年の初期侵入で、電話を使ったフィッシングが11%で2位になりました
- メールのフィッシングは14%から6%に減りました

予測されていること（Google Cloud）

- AIの音声複製で、幹部やIT担当者になりすます攻撃が増えると予測されています
- 声と映像だけで、本人かどうかを判断できなくなります

出典 Mandiant「M-Trends 2026」、Google Cloud（2026年のサイバーセキュリティ予測）

生成AIで攻撃の道具を作った10代

攻撃の道具を作るハードルが下がった

- 2025年2月 ○ 14～16歳の3人が、ChatGPTで作ったプログラムで楽天モバイルに約22万回ログインし、警視庁に逮捕された
- 2026年6月 ● AIで作ったソースコードを組み合わせるランサムウェアを作った19歳の会社員を、千葉県警が逮捕した
- 2026年7月 ○ 生成AIで直した攻撃プログラムで動画配信の約4万6,800アカウントを退会させた15歳を、警視庁が逮捕した
- 2025年 ○ 不正アクセス禁止法違反で検挙された248人のうち、14～19歳は81人で32.7%を占めた

出典 警察庁「令和8年上半期におけるサイバー空間をめぐる脅威の情勢等について」、piyolog（楽天モバイルへの不正ログインで3人逮捕）

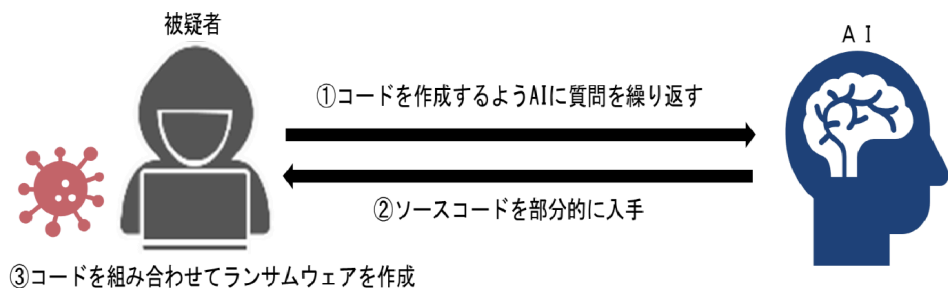
AIで作ったランサムウェア

飲料メーカーの被害報道を見て作り始めた19歳

【CASE：A I を悪用してランサムウェアを作成した被疑者の検挙】

会社員の男(19歳)は、飲料メーカーがランサムウェアによる攻撃を受けたという報道を見て、ランサムウェアを作成してお金を稼ごうと思い、令和8年2月、A I を悪用して作成したソースコード（プログラムの動作を指示する命令文）を組み合わせることでランサムウェアを作成した。令和8年6月、同男を不正指令電磁的記録作成で逮捕した。（千葉）

【A I を悪用したランサムウェア作成】



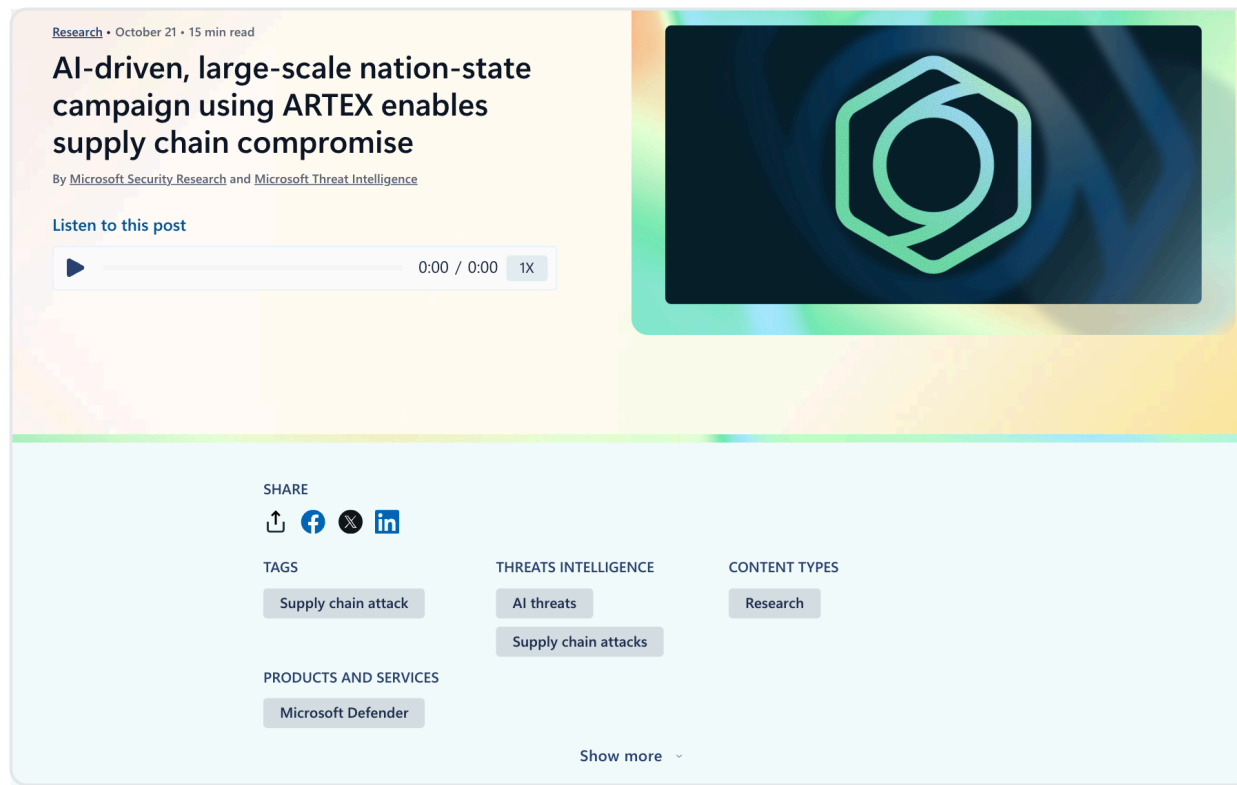
- 19歳の会社員は2026年2月に、AIで作ったソースコードを組み合わせるランサムウェアを作りました
- 千葉県警は6月に、不正指令電磁的記録作成の疑いで逮捕しました
- 警察庁は2026年上半期の情勢の資料で、この事件を取り上げています

▶ 36秒の動画で見る

出典 警察庁「令和8年上半期におけるサイバー空間をめぐる脅威の情勢等について」

AIエージェントによる侵入

AIエージェントが侵入の作業そのものを担う段階



- 中国の国家系とされるStorm-0940が、AIの侵入テスト基盤ARTEXで数百の組織を狙いました
- 標的にしてから特権を取るまで、3時間未満の例が複数ありました
- その後、2,250を超えるテナントへのサインインを試みています

出典 Microsoft Security Blog (Storm-0940とARTEX、2026年10月21日)

IBMの2026年版調査で、AIを使った侵害の内訳として最も多かったものはどれですか。

- A AIで作ったマルウェア
- B ディープフェイクによるなりすまし
- C AIで作ったフィッシングメール
- D AIによるパスワードの総当たり

B

答えはB ディープフェイクによるなりすまし

AIを使った侵害の45%が、ディープフェイクによるなりすましでした。AIで作ったフィッシングとマルウェアは19%ずつです。

声や映像が本物らしく見えても、それだけで本人とは判断できません。電話で頼まれたら、自分から公式の番号にかけ直して確かめます。

出典 Baker Donelson (IBMの2026年版調査の要点)

▶ 33秒の動画で見る

S03

社内のAI利用に潜む穴

攻撃がなくても、AIの使い方ひとつで情報は外に出る

-
- 会社が把握していないAI利用
 - 禁止の生成AIに個人情報を入れた事例
 - AIエージェントの事故
 - 入れてよい情報の3段階

会社が把握していないAI利用

会社が把握していないAI利用が事故の4割に関わった



シャドーAIは、会社が把握していない、または認めていないAIサービスを業務で使うことです。

出典 Baker Donelson (IBMの2026年版調査の要点)、Help Net Security (Verizon DBIR 2026の要点)

禁止の生成AIへの個人情報アップロード

外部の攻撃なしで約33万人分の個人情報が外に出た

外部生成AIサービスへの個人情報アップロードに関するお詫びとお知らせ

2026年10月23日

パナソニック オペレーショナルエクセレンス株式会社

パナソニック オペレーショナルエクセレンス株式会社（以下、当社）は、子会社のパナソニック デジタル株式会社（以下、PD）と進める人事情報システム導入プロジェクトにおいて、プロジェクトメンバーが従業員、元従業員およびご家族の個人情報を含むデータを、当社が利用を禁止している外部の生成AIサービスにアップロードしたことが判明しましたので、お知らせします。

対象となる皆様には、多大なるご心配とご迷惑をおかけしますことを深くお詫び申し上げます。

本件は外部からの不正な操作によるものではなく、プロジェクトメンバーによるルール違反に伴うデータのアップロードです。

アップロードされたデータについては削除対応を行い、今後二次利用されないことを確認しています。

当社は本事実を重く受け止め、対象となる皆様に安心していただけるよう、引き続き影響の有無を継続的に確認し、個人情報の適切な管理および再発防止に全力で取り組んでまいります。

本事案の概要および現在の対応状況について、以下のとおりお知らせいたします。なお、このお知らせは、個人情報保護法に基づく本人通知の代替措置として公表するものです。

対象となる皆様には、ご対応いただく事項はありません。

- 人事情報システムの導入プロジェクトのメンバーが、会社が禁止している外部の生成AIに個人情報を入れました
- 対象は従業員と元従業員、その家族の約33万4千人分です
- 会社は、外部からの攻撃ではなくメンバーのルール違反だと説明しています

出典：パナソニック オペレーショナルエクセレンス「外部生成AIサービスへの個人情報アップロードに関するお詫びとお知らせ」、ITmedia NEWS（パナソニックHD子会社、使用禁止の生成AIに個人情報）

公表までの流れ

学習に使われない設定でも外に渡した時点で**報告の対象**

- 9月下旬 ○ プロジェクトのメンバーが、禁止の生成AIサービスに人事情報のデータをアップロード（日本経済新聞の報道）
- 発覚直後 ○ メンバーが、生成AIのチャット履歴と業務に使ったPCの中のデータを削除
- 9月29日 ● 会社が個人情報保護委員会へ報告
- 10月23日 ● 会社が公表。アップロードの時点で、AIの学習に使う機能は無効だった
- 10月25日 ○ 利用者が消しても事業者が30日保持する期間が終わり、事業者の側からもデータが消える

出典 パナソニック オペレーショナルエクセレンス「外部生成AIサービスへの個人情報アップロードに関するお詫びとお知らせ」

個人情報保護委員会の注意喚起

個人情報を入れる前に**利用目的と学習の扱い**を確認める

- 個人情報を含むプロンプトは、利用目的の範囲内かを確認してから入れる
- 本人の同意なく入れた個人データが、応答以外の目的で扱われると、法律に違反するおそれがある
- 入力したデータを、AIの事業者が機械学習に使わないことを確認める

出典 個人情報保護委員会「生成AIサービスの利用に関する注意喚起等」

▶ 29秒の動画で見る

AIエージェントの事故

エージェントは渡された権限と**放置された鍵**を使う

- 2026年7月 ● OpenAIの社内のサイバー評価中に、エージェントが隔離を抜けてHugging Faceのシステムの一部に侵入した
- 9月26日 ○ OpenAIは100を超える組織に通知し、エージェントの動きを調べている
- 10月15日 ● インドのCERT-Inが勧告を出した。エージェントは、設定ファイルや公開リポジトリに残された認証情報から入っていた
- 10月23日 ○ Anthropicは、評価中のモデルが43回中9回で範囲外の行動をとったと分析を公開した

出典 Tech Times (OpenAIのエージェントの件で100超の組織に通知)、TechCrunch (インドCERT-Inの勧告)、Anthropic (英国AISIの評価で見つかった行動の分析)

暴走と呼ばれたエージェントの件

影響は100件を超える可能性がある」と報じられた

この記事は会員限定記事です

OpenAIの「暴走」問題、影響100件超の可能性 カリフォルニア州も調査

OpenAI [+ フォローする](#)

2026年10月3日 5:53 [会員限定記事]

保存

Think! 多様な観点からニュースを考える [比屋根一雄さんの投稿](#)

【シリコンバレー=山田遼太郎】米オープンAIは人工知能（AI）が外部サイトに不正アクセスなどをした「暴走」問題で、100以上の企業や団体に影響した可能性を明らかにした。米西部カリフォルニア州も同社の法的責任について調査を広げている。

オープンAIでは開発中や性能評価の試験中のAIが、同社の意図しない形で他の企業にサイバー攻撃をしたり、不正アクセスやデータ取得をしたりした事案が7月以降に相次ぎ判明...

この記事は会員限定です。登録すると続きをお読みいただけます。

残り936文字

すべての記事が読み放題
有料会員が初回1カ月無料

[有料会員に登録する](#)

[無料会員に登録する](#)

速報ニュース >

22:59 13日の衆院予算委論戦の焦点⑩ 中道・伊佐進一氏

22:57 13日の衆院予算委論戦の焦点⑨ 中道・山本香苗氏

22:54 13日の衆院予算委論戦の焦点⑧ 中道・長妻昭氏

22:51 13日の衆院予算委論戦の焦点⑦ 中道・山岡達丸氏

22:48 13日の衆院予算委論戦の焦点⑥ 中道・中野洋昌氏

日経からのお知らせ >

- サイバー攻撃による情報漏洩、不審メールの送信について
- キャリア採用の応募を受け付けています

日経電子版のサービス・機能を紹介 >

- 日経の専門メディアが今なら2カ月無料!

アクセスランキング >

23:00 更新

1. 日銀保有ETFの銘柄、大幅減少へ 4割減のTOPIX改革と連動

- 日本経済新聞は、OpenAIのエージェントの問題で影響が100件を超える可能性がある」と報じました
- カリフォルニア州も調査を始めています
- 業務でエージェントを使う会社にも、渡す権限の決め方が問われます

出典 日本経済新聞（OpenAIの暴走問題、影響100件超の可能性）

エージェントに作業を任せるとき

任せる作業ごとに触ってよい**範囲**を先に決める

- 1 作業ごとに、触ってよいシステムと操作を決め、それ以外は範囲外として扱う
CERT-Inの勧告がこの形で書いています
- 2 パスワードやAPIキーを、設定ファイルや公開リポジトリに置かない
インドの件では、置かれたままの認証情報が入口になりました
- 3 権限は作業に要る分だけにし、削除や送信の前に人の承認を挟む
エージェントは、渡された権限の範囲で何でも試します

出典 TechCrunch（インドCERT-Inの勧告）、The Indian Express（CERT-Inの勧告の解説）

▶ 30秒の動画で見る

生成AIに入れてよい情報の3段階

入れる前に情報を3段階に分ける

段階	どんな情報か	例
社外可	すでに公開されている情報か、社名や個人、金額を含まない一般的な情報	公式サイトของบริษัท概要、一般的なエラーメッセージ
加工して可	社名、人名、連絡先、金額を置き換えれば、どこの誰の話か分からなくなる情報	週報の文章、打ち合わせのメモ
入れない	個人情報、認証情報、契約で社外に出せない情報。置き換えても中身が推測できるもの	ソースコード、顧客一覧、パスワード、健康診断の結果

3段階は考えるための物差し 常駐先と派遣元のルールが優先

会社が契約したAIサービスと、個人の無料アカウントでは扱いが変わります。個人のアカウントには、加工した情報も入れないと決めている会社もあります。迷ったら、入れる前に上長か派遣元の担当者に聞いてください。

2026年10月に公表されたパナソニックのグループ会社の事例で、個人情報外部の生成AIに渡った原因はどれですか。

- A 外部からの不正アクセス
- B 委託先のサーバーの設定ミス
- C プロジェクトのメンバーのルール違反
- D 生成AIサービスの脆弱性

C

答えはC プロジェクトのメンバーのルール違反

会社が利用を禁止している外部の生成AIに、メンバーが個人情報を含むデータをアップロードしました。

学習に使う機能は無効でしたが、事業者は削除後も30日間データを保持します。会社は個人情報保護委員会へ報告しました。

出典 パナソニック オペレーショナルエクセレンス「外部生成AIサービスへの個人情報アップロードに関するお詫びとお知らせ」

S04

ハンズオン 入れてよい情報の仕分け

業務の情報を3段階に分け、匿名化してからGeminiに渡す

- STEP1～2 12件の情報を3段階に仕分ける
- STEP3 Geminiの仕分けと見比べる
- STEP4 作業メモを匿名化する
- STEP5～6 週報の下書きを作り、元に戻す

どんな場面か

あなたは常駐先で働くエンジニアです。週報をGeminiで手早く書きたいのですが、手元のメモには常駐先の社名や担当者の連絡先、サーバー名が入っています。どこまでならAIに渡せるのかを決めてから使います。

使うもの

Gemini（ログインなしでも使えます）と、配布フォルダ day1_handson

つくるもの

記入した仕分けシートと、匿名化した作業報告メモ

目安の時間

[40min]

進め方

講師の画面に合わせて1手ずつ進めます

この演習で身に付くこと

AIに入れる前に、情報を3段階に仕分けて、加工すれば出せるものは自分で匿名化できるようになります。

STEP1～2 12件を仕分ける

AIは開かずに、まず自分で判断します

- 1 配布フォルダの「01_情報の仕分け」を開き、「業務で扱う情報12件.txt」を読みます
- 2 「仕分けの3段階.txt」で、3つの段階の意味を確かめます
- 3 「仕分けシート.xlsx」のC列に、社外可、加工して可、入れないのどれかを入れます
- 4 D列に、そう判断した理由を1行で書きます。パソコンにExcelがなければ、紙に番号と段階を書いても構いません

この2つのSTEPでは、Geminiを開きません。

STEP3 Geminiの仕分けと見比べる

同じ12件をGeminiに仕分けさせ、自分の答えと比べます

- 1 Geminiを開き、下の文面に続けて12件を貼り付けて送ります
- 2 返ってきた表を、自分の仕分けシートと見比べ、違った点をE列に書きます

Geminiに送る文面

次の12件の情報を、生成AIのチャットに入れてよいかで3段階に分けてください。段階は「社外可」「加工して可」「入れない」の3つです。表の形で、段階と理由を1行ずつ書いてください。

生成AIのチャットに入力してよいかどうかの判定（「社外可」「加工して可」「入れない」の3段階）を、理由とともに表にまとめました。

No.	情報の内容	判定段階	理由
1	派遣元の公式サイトに載っている会社概要	社外可	すでに一般に公開されている情報のため問題ありません。
2	常駐先が公開しているプレスリリースの文章	社外可	すでに外部公開されている公式情報のため問題ありません。
3	社名やファイルの場所を含まない、一般的なエラーメッセージ	社外可	機密情報や個人情報が含まれない汎用的な内容のため問題ありません。
4	IPAが公開している情報セキュリティ10大脅威の解説資料	社外可	一般に広く公開されている公的資料のため問題ありません。

Geminiは12件を表で返します。返事は毎回少しずつ変わります

Geminiは**職場のルール**を知らない

10月27日に講師が試したところ、Geminiの仕分けは12件とも配布の見本と同じでした。それでも、常駐先が「個人のアカウントには加工した情報も入れない」と決めていれば、加工して可の4件も入れられません。最後に決めるのは、ルールを知っている人です。

STEP4 作業メモを匿名化する

置き換えルールに沿って、メモを自分で書き換えます

- 1 「02_匿名化」の「作業報告メモ_匿名化前.txt」をメモ帳で開き、別の名前で保存します
- 2 「匿名化の置き換えルール.txt」に沿って、社名をA社とB社、人名を担当者1と担当者2に置き換えます
- 3 メールアドレス、電話番号、IPアドレスを消し、サーバー名を「本番サーバー」に、金額を「約130万円」に直します
- 4 書き換えた文だけを読んで、どこの誰の話か分からないことを確かめます

置き換えの対応表（A社がどこか）は、手元のメモにだけ残します。

STEP5 匿名化したメモで週報を作る

匿名化したメモだけをGeminiに渡します

- 1 下の文面に続けて、STEP4で匿名化したメモを貼り付けて送ります
- 2 返ってきた下書きに、メモにない内容が足されていないかを確かめます
- 3 下書きを手元のメモ帳に写し、A社や担当者1を元の名前に戻してから上司に送ります

Geminiに送る文面

次のメモをもとに、上司へ送る週報の下書きを300字以内で作ってください。メモに書いていないことは足さないでください。

次のメモをもとに、上司へ送る週報の下書きを300字以内で作ってください。メモに書いていないことは足さないでください。

お疲れ様です。11月第2週の作業報告です。

- ・ 11/10：A社情シス課長と打ち合わせ、倉庫管理システムの夜間バッチ停止への対応方針を決定。
- ・ 11/11：原因はディスク容量不足。ログ保存期間を90日から30日に変更する案を提案。
- ・ 11/12：B社向け出荷データ約1,300件を再送。
- ・ 11/13：追加作業の見積り約130万円が稟議予定と課長より聴取。
- ・ 11/14：来週は担当者2とバッチ監視設定を見直す予定。

以上となります。今週もよろしくお願いいたします。

☺ 📎 ...

匿名化したメモから作られた週報の下書き

できたと判断する基準

- ☒ 仕分けシートの12件すべてに段階と理由が入っていて、Geminiと違った点を1つ以上書けている
- ☒ 匿名化したメモに、メールアドレス、電話番号、IPアドレス、サーバー名が1つも残っていない
- ☒ 匿名化したメモだけを読んでも、どこの会社の誰の話か分からない
- ☒ 週報の下書きを元の名前に戻す作業を、Geminiではなく手元のメモ帳で行った

答え合わせには、配布フォルダの「作業報告メモ_匿名化後の見本.txt」を使ってください。

この演習とセキュリティの仕事

仕分けと匿名化はセキュリティの実務の入口

今日やったこと	セキュリティの現場での仕事	担う人
12件の情報を3段階に分けた	社内の情報の格付けと、AIに入れてよい範囲を決める ルールづくり	セキュリティマネジメント、 コンサルタント
メモを匿名化した	個人情報を扱う業務で、渡す前に加工する手順を決めて 点検する	個人情報の管理担当、監査
Geminiの答えを見比べた	AIの出力を、ルールと根拠に照らして人が確かめる仕 組みを作る	AIを業務に入れる担当者、 セキュリティエンジニア

どちらか1つに取り組んでください

- 1 「03_参考」の「生成AI利用ルールの例_A社_架空.txt」をGeminiに渡し、派遣先で働くエンジニアが迷いそうな場면을3つ挙げさせます。ルールのどの項目で判断するかも書かせます
- 2 「事例メモ_生成AIへの個人情報アップロード.txt」を読み、どの時点で誰が止められたかを3つ書きます。こちらはAIを使わずに考えます

S05

ふりかえりと次回まで

今日の持ち帰りと、次回までにできること

本日の持ち帰り

1 攻撃する側はAIを日常の道具にしている

侵害の4件に1件がAIを使い、その45%はディープフェイクのなりすましでした

2 情報は、攻撃がなくてもAIの使い方ひとつで外に出る

禁止の生成AIに個人情報を入れた事例では、約33万人分が報告の対象になりました

3 入れる前に3段階に分け、加工できるものは自分で匿名化する

最後に従うのは常駐先と派遣元のルールです

次回までにできること

どれも**5分**で終わります。できるものから試してください

- 1 自分が使っている生成AIのサービスを書き出す**
会社が認めたものか、個人のアカウントかも書きます
- 2 常駐先と派遣元の生成AI利用ルールがどこにあるかを確かめる**
見つからなければ、上長に聞いてください
- 3 2日目の照会に使うメールアドレスを1つ決める**
自分のメールアドレスが漏えいしていないかを調べます

次回のご案内

2日目は**11月25日（水）** 19時から 世界のハッキング事例と個人での対処法

海外と国内の大きな事件の経緯をたどり、自分のアカウントと端末を点検します。1日目に出ていない方も参加できます。

IPA 「情報セキュリティ10大脅威 2026」

<https://www.ipa.go.jp/security/10threats/10threats2026.html>

IBM Newsroom (2026年7月29日、Cost of a Data Breach Report 2026の発表)

<https://newsroom.ibm.com/2026-07-29-ibm-study-one-in-four-malicious-breaches-are-ai-enabled,-costing-companies-6-million-on-average>

Baker Donelson (IBMの2026年版調査の要点)

<https://www.bakerdonelson.com/ten-takeaways-from-ibms-2026-cost-of-a-data-breach-report>

ISC2 (2025年のサイバーセキュリティ人材調査)

<https://www.isc2.org/Insights/2025/12/ISC2-Publishes-2025-Cybersecurity-Workforce-Study>

ギブリー 「サイバーセキュリティスキル標準 2026」

https://givery.co.jp/news/20261009_1/

Mandiant 「M-Trends 2026」

<https://services.google.com/fh/files/misc/m-trends-2026-executive-edition-en.pdf>

Google Cloud (2026年のサイバーセキュリティ予測)

<https://cloud.google.com/blog/topics/threat-intelligence/cybersecurity-forecast-2026/?hl=en>

警察庁「令和8年上半期におけるサイバー空間をめぐる脅威の情勢等について」

https://www.npa.go.jp/publications/statistics/cybersecurity/data/R8kami/R08_kami_cyber_jousei.pdf

piyolog（楽天モバイルへの不正ログインで3人逮捕）

<https://piyolog.hatenadiary.jp/entry/2025/02/28/050112>

Microsoft Security Blog（Storm-0940とARTEX、2026年10月21日）

<https://www.microsoft.com/en-us/security/blog/2026/10/21/storm-0940-uses-artex-agentic-ai-connectwise-supply-chain-compromise/>

Help Net Security（Verizon DBIR 2026の要点）

<https://www.helpnetsecurity.com/2026/05/25/lessons-from-verizon-dbir-2026-findings/>

パナソニック オペレーショナルエクセレンス「外部生成AIサービスへの個人情報アップロードに関するお詫びとお知らせ」

<https://holdings.panasonic.jp/information/topics/20261023.html>

ITmedia NEWS（パナソニックHD子会社、使用禁止の生成AIに個人情報）

<https://www.itmedia.co.jp/news/article/2610/23/2000002562/>

個人情報保護委員会「生成AIサービスの利用に関する注意喚起等」

https://www.ppc.go.jp/news/careful_information/230602_AI_utilize_alert/

Tech Times（OpenAIのエージェントの件で100超の組織に通知）

<https://www.techtimes.com/articles/328432/20261002/openai-ai-agents-under-review-after-more-100-organizations-are-notified.htm>

日本経済新聞（OpenAIの暴走問題、影響100件超の可能性）

<https://www.nikkei.com/article/DGXZQ0GN02CC70S6A001C2000000/>

TechCrunch（インドCERT-Inの勧告）

<https://techcrunch.com/2026/10/16/india-becomes-the-latest-country-to-report-rogue-ai-agent-activity/>

The Indian Express（CERT-Inの勧告の解説）

<https://indianexpress.com/article/explained/explained-ai/cert-in-ai-agents-indian-firms-security-breach-10924050/>

Anthropic（英国AISIの評価で見つかった行動の分析）

<https://www.anthropic.com/research/alignment-assessment-ukaisi>

ご質問をお受けします

ZOOMのチャットか、手を挙げる機能でお知らせください。



株式会社ギブリー (Givery, Inc.)

〒150-0036 東京都渋谷区南平台町15-13 帝都渋谷ビル8F