共催：CoWorker The Digital Improvement Studio　GSX GLOBAL SECURITY EXPERTS

【CoWorker株式会社／GSX共催ウェビナー】

AI活用を止めないためのセキュリティ戦略
～AI時代の攻撃・防御・ガバナンスを考える～

参加費 無料

2026年7月16日 木　11:00～12:00（10:45開場）

定員50名

※ 事前登録制につき定員になり次第、受付を終了させていただきます。
※タイムスケジュール、講演内容、講演者等は、予告なく変更される場合がございます。ご了承ください。

AI活用を推進したい一方で、情報漏えい、シャドーAI、プロンプトインジェクション、AIエージェントの権限管理などに課題を感じている企業の皆さまに向けて、実務で押さえるべき考え方をお伝えします。生成AIの登場により、企業の業務効率化や新たな価値創出の可能性は大きく広がっています。一方で、AIは防御側だけでなく攻撃側にも利用され、フィッシング、偵察、脆弱性探索、マルウェア開発など、さまざまな攻撃活動の効率化に使われ始めています。

また、社内での生成AI活用が進むにつれ、機密情報の入力、意図しない情報漏えい、プロンプトインジェクション、外部サービスとの連携リスク、AI利用ルールの未整備といった新たな課題も顕在化しています。

AI時代のセキュリティでは、攻撃の進化に備える防御策と、AIを安全に活用するためのガバナンスの両方が欠かせません。

本ウェビナーでは、AIを悪用する攻撃の最新動向と防御の考え方、そして企業がAI活用を止めずに安全性を確保するための実践ポイントを、Coworker社とGSXの両視点から解説します。

オープニング

開会のご挨拶

グローバルセキュリティエキスパート株式会社　管理本部　マーケティング部

セッション1

11:05-11:30
(25分)

AI vs AI のセキュリティ時代　～攻撃側の進化と、防御の考え方～

CoWorker株式会社
代表取締役　山里 一輝 氏
執行役員CSO　伊藤 達哉 氏

AIの進化は、企業の業務効率化だけでなく、サイバー攻撃の手法にも大きな変化をもたらしています。攻撃者はAIを活用することで、偵察、標的選定、フィッシングメールの作成、脆弱性探索、攻撃シナリオの自動化などを効率化し、従来よりも速く、巧妙な攻撃を実行できるようになりつつあります。

本セッションでは、AIを活用した攻撃の進化と、それに対抗するための防御の考え方について解説します。AI時代におけるセキュリティ運用の変化、Blue Agent、Red Agent、Purple Agent、AIDRなどのアプローチを通じて、攻撃者のAI活用にどのように備えるべきかを紹介します。

攻撃側も防御側もAIを活用する時代において、企業はどのような視点で脅威を捉え、どのような防御体制を構築すべきか。その実践的なヒントをお届けします。

裏面に続く

セッション2

11:30-11:55
(10分)

生成AIを安全に使うためのセキュリティガバナンス
～AI活用を止めないために、企業が整備すべきリスク管理と実践ポイント～

グローバルセキュリティエキスパート株式会社
サイバーセキュリティ事業本部 事業推進部
副部長 安川 琢

生成AIの業務利用が広がる中、多くの企業では「どこまで利用を認めるべきか」「どのような情報を入力してよいのか」「AI利用に伴うセキュリティリスクをどう管理すべきか」といった課題が生まれています。

AI活用を推進するうえで重要なのは、利用を一律に禁止することではなく、リスクを把握したうえで安全に活用できるルール、体制、技術的対策を整備することです。

本セッションでは、生成AI利用に伴う代表的なリスクとして、機密情報の漏えい、シャドーAI、プロンプトインジェクション、RAGやAIエージェント利用時のリスク、社内ルール未整備による統制不全などを取り上げます。

そのうえで、企業が取り組むべきAIセキュリティガバナンスのポイントとして、利用ルールの策定、データ分類、リスクアセスメント、セキュリティレビュー、ログ管理、教育・啓発、継続的な見直しの考え方を解説します。

GSXは、企業がAI活用を止めることなく、安全かつ現実的に利用を進めるためのセキュリティ対策とガバナンス整備の実践ポイントをお伝えします。

Q&A

11:55-12:00
(5分)

オンラインでQ&Aを実施します。
講演中に「Q&A」から発信されたご質問に対して講演後にご回答させていただきます。

■Webからのお申込み及び詳細について

https://www.gsx.co.jp/seminar/webinar_260716.html

【個人情報のお取扱いについて】
グローバルセキュリティエキスパート株式会社（以下「当社」といいます）はプライバシーポリシーに基づき、お客様の個人情報の取扱いに細心の注意を払っております。当社における個人情報の取扱いについての考え方を以下に記載します。

■個人情報の収集について
当社では次のような場合にお客様の個人情報をお聞きします。
1. 会員制サービスにご登録いただく場合
2. 各種セミナー等にお申し込みいただく場合
3. アンケートにお答えいただく場合

お客様はご自身の個人情報を明らかにすることなく当社のホームページをご利用いただけますが、一部のページへのアクセスおよび一部のサービスのご利用ができない場合がございますのでご了承下さい。

■個人情報の利用について
当社にご提供いただいたお客様の個人情報は、次のような目的の達成に必要な範囲内においてのみ利用いたします。
1. 申し込まれたサービスの提供のため
2. 申し込まれたサービス関連情報の提供のため
3. お問い合わせに対する対応のため
4. サービスの企画・向上のため
5. お客様に有用な情報を提供するため

■個人情報の管理について
当社は、お客様の個人情報の紛失、破壊、改ざん、漏えいなどが起こらないよう適切な安全管理策を実施し、厳重に管理します。

■個人情報の第三者への提供について
当社は、個人情報をお客様の承諾なしに第三者に提供することはありません。
なお、以下の場合は除きます。
1. 個人情報の取扱い業務の一部を社外に委託する場合
2. 裁判所など法令の定める事務を遂行することに対して協力する場合

■個人情報の問い合わせについて
お客様は当社に対し、当社が管理しているお客様の個人情報を問い合わせることができます。
個人情報の開示、訂正、削除を要求される場合またはその他お客様の個人情報に関するお問い合わせは、下記のお客様情報相談窓口までご連絡下さい。

GSX
GLOBAL SECURITY EXPERTS

グローバルセキュリティエキスパート株式会社
管理本部
〒105-0022　東京都港区海岸1-16-1 ニューピア竹芝サウスタワー10F
TEL：03-3578-9001　FAX：03-3578-9020　Mail：salesall@gsx.co.jp