



2026 年 10 月 15 日

各 位

会 社 名	ポ ー ル ト ウ ウ イ ン ホ ー ル デ ィ ン グ ス 株 式 会 社
代表者名	代表取締役社長 橘 鉄 平 (コード番号：3657 東証プライム)
問合せ先	取締役 CFO 山 内 城 治 (Email：ir@ptw.inc)

当社連結子会社による新サービス提供開始に関するお知らせ ～生成 AI 活用を安全面から支援する「生成 AI 利活用セキュリティ支援サービス」を提供開始～

当社の連結子会社である株式会社 SynX（本社：東京都千代田区、代表取締役：西 潤一郎、以下「SynX」）は、企業における生成 AI の安全な利活用を支援する「生成 AI 利活用セキュリティ支援サービス」（以下「新サービス」）の提供を開始いたしましたので、お知らせいたします。

生成 AI は、企業データや業務プロセスと連携する経営インフラとして日々急速に普及しており、自律的に業務を実行する AI エージェントへの注目も高まっています。一方で、情報漏えいリスクや従業員による未承認の生成 AI 利用（シャドーAI）への対応、アクセス権管理、AI 固有のセキュリティリスクへの対策等、安全な利活用を支えるガバナンス体制の整備が重要な経営課題となっています。

脆弱性診断サービスの提供を通じて、セキュリティリスク分析・対策支援の知見を培ってきた SynX は、このような背景のもと、新サービスの提供を開始いたしました。新サービスは、生成 AI の利用状況やリスクを可視化する「生成 AI セキュリティアセスメント」と、その結果に基づき AI ガバナンス体制や情報保護対策の構築を支援する「生成 AI ガバナンス・セキュリティ構築」の2つのサービスで構成されます。AI 利用ガイドラインの策定、DLP、ID・アクセス管理、教育・インシデント対応等を包括的に支援し、企業の AI 活用とリスク管理の両立を実現します。

企業における生成 AI 及び AI エージェント活用の拡大に伴い、関連するセキュリティ需要の拡大が見込まれます。SynX は本サービスを起点に実績とサービス基盤を強化し、将来的には AI アプリケーション向けセキュリティ診断や、AX（AI トランスフォーメーション）支援サービス等へ事業領域を拡大する方針です。当社グループは、AI 活用を支えるセキュリティ領域から業務変革支援まで一貫したサービス提供体制を構築し、企業の AI 活用を包括的に支援してまいります。

ゲームデバッグにおいて国内トップクラスのシェアを有する当社グループは、非ゲームのソフトウェアテストを中心とした国内 Tech 分野を成長領域の1つに位置付けております。本件が当社の業績に与える影響は、現時点では軽微であると考えておりますが、中長期的には収益基盤の強化に寄与するものと考えております。

新サービスの詳細な内容については、添付資料をご参照ください。

■SynX、企業の生成 AI 活用を安全面から支援する「生成 AI 利活用セキュリティ支援サービス」を提供開始
脆弱性診断で培った知見を活かし、企業が生成 AI を「安全に使う」ための体制づくりを支援

以 上

SynX、企業の生成 AI 活用を安全面から支援する
「生成 AI 利活用セキュリティ支援サービス」を提供開始
～脆弱性診断で培った知見を活かし、企業が生成 AI を「安全に使う」ための体制づくりを支援～

株式会社 SynX（代表取締役：西 潤一郎、本社：東京都千代田区、主要株主：ポールトゥウィンホールディングス株式会社（100%）、東京証券取引所プライム市場上場（証券コード：3657）、以下 SynX）は、企業における生成 AI の安全な利活用を支援する「生成 AI 利活用セキュリティ支援サービス」の提供を開始したことをお知らせします。



本サービスでは、SynX がこれまでセキュリティ脆弱性診断で培ってきたセキュリティ評価の知見を活かし、生成 AI セキュリティ領域へ事業を拡大します。SynX は、「生成 AI を使わせないためのセキュリティ」ではなく、「生成 AI を安全に使うためのセキュリティ」という考え方のもと、利用促進とリスク管理を両立する仕組みづくりを支援します。

■ サービス開始の背景

生成 AI は「個人利用」から「企業の業務基盤」へと移行しつつあります。文章作成や検索支援にとどまらず、社内情報の検索、資料作成、開発、顧客対応、RAG、AI エージェントなど、企業データや業務プロセスと接続する段階へ進んでいます。

これに伴い、生成 AI の課題は「AI ツールを利用してよいか」ではなく、「どの情報を、誰が、どの AI から、どこまで利用できるようにするか」という、企業の情報管理・アクセス管理の問題へと変化しています。企業における生成 AI の利活用が進む一方で、次のようなセキュリティ・ガバナンス上の課題も生じています。

- 機密情報・個人情報・顧客情報・ソースコード・社内資料などを AI へ入力することによる**情報漏えいリスク**
- 会社が把握していない生成 AI や個人アカウント、無許可の AI サービスが業務で利用される「シャドーAI」
- 生成 AI が社内データと連携することで、従来は利用者が探せなかった情報まで AI が検索・要約する可能性があるため、**元データのアクセス権設計が重要となること**
- プロンプトインジェクション、機密情報開示、過剰な権限付与（Excessive Agency）、RAG／ベクトル関連、AI サプライチェーンなど、**従来型の Web システムとは異なる AI 固有のセキュリティリスクへの対応**

また、生成 AI の利用を禁止しても、従業員が外部 AI サービスを利用することで、企業側が利用状況を把握できない「シャドーAI」につながる可能性があります。さらに、生成 AI のリスクはセキュリティ部門だけの問題ではなく、情報システム、法務・コンプライアンス、データ管理、人事・教育、事業部門など、複数の部門に関係します。

そのため企業には、「ChatGPT を禁止する」「Copilot を導入する」といった個別の判断にとどまらず、誰が管理するのか、何を利用可能とするのか、どのデータを入力できるのか、新しい AI サービスをどう審査するのか、事故発生時にどう対応するのかまでを含めた「AI ガバナンス設計」が必要とされています。

OWASP GenAI Security Project では、LLM や生成 AI、AI エージェントなどについて、プロンプトインジェクション、機密情報開示、過剰な権限付与（Excessive Agency）などの重要なセキュリティリスクが体系化されています。

また、NIST の AI Risk Management Framework（AI RMF）では、Govern・Map・Measure・Manage という、組織的な AI リスク管理の考え方が示されています。こうした背景を踏まえ、SynX は既存のセキュリティ脆弱性診断で培った知見を活かし、生成 AI を安全に利活用するためのセキュリティ支援サービスを開始します。

■ 「生成 AI 利活用セキュリティ支援サービス」の概要

本サービスは、企業における生成 AI の利用状況やセキュリティ・ガバナンス上の課題を可視化する「生成 AI セキュリティアセスメント」と、発見した課題に対して具体的な改善を支援する「生成 AI ガバナンス・セキュリティ構築」の 2 つのサービスを提供します。

・STEP 1：生成 AI セキュリティアセスメント

顧客企業の生成 AI 利用状況を把握し、セキュリティ・ガバナンス上のリスクと改善ポイントを可視化します。生成 AI の利用状況とデータの扱い、情報漏えいリスク、ID／アクセス権、利用ルール／体制を評価し、改善ロードマップとしてご提示します。

・STEP 2：生成 AI ガバナンス・セキュリティ構築

STEP 1 で発見した課題に対して具体的な改善支援を行い、安全に生成 AI を利活用できる環境を構築します。

主な支援内容

- ・ AI 利用ガイドライン
- ・ AI ガバナンス体制
- ・ 情報保護・DLP
- ・ ID・アクセス管理
- ・ 教育・インシデント対応

■ セキュリティ脆弱性診断で培った知見を生成 AI 領域へ

SynX はこれまで、Web、Mobile、Network、Cloud、IoTなどを対象としたセキュリティ脆弱性診断サービスを提供してきました。本サービスでは、これまでのセキュリティ評価ノウハウを活かし、生成 AI セキュリティ領域へ支援範囲を広げます。

従来の「脆弱性を発見する」セキュリティ診断を起点に、生成 AI の利用状況や課題を可視化するアセスメント、さらにガバナンス・セキュリティ構築まで、企業の生成 AI 利活用におけるセキュリティ課題を段階的に支援します。

既存のセキュリティ脆弱性診断をご利用のお客様には、診断を通じて把握したシステム環境や課題を踏まえ、生成 AI 利活用に関するセキュリティ支援をご提案することも可能です。

サービスメニュー

サービス	価格
生成 AI セキュリティアセスメント	100 万円～
生成 AI ガバナンス・セキュリティ構築	200 万円～

※価格は対象範囲・内容により変動します。詳しくはお問い合わせください。

■ サービス提供の流れ

本サービスは、SynX のセキュリティ脆弱性診断を起点とした、次の流れで提供します。

①生成 AI 利用状況のヒアリング

生成 AI の利用状況、データの取り扱い、利用ルール・管理体制などを確認します。

②セキュリティ・ガバナンス上の課題を可視化

生成 AI の利活用に伴うセキュリティ・ガバナンス上のリスクと改善ポイントを整理します。

③改善ロードマップのご提案

評価結果をもとに、優先すべき課題や改善の方向性をご提示します。

④ガバナンス・セキュリティ構築

必要に応じて、AI 利用ガイドライン、ガバナンス体制、情報保護・DLP、ID・アクセス管理、教育・インシデント対応などの整備を支援します。



生成 AI 利活用セキュリティ支援サービス提供の流れ（①～④）

■ SynX が目指す生成 AI セキュリティの在り方

SynX は、生成 AI を「禁止すべきリスク」ではなく、「安全に活用することで事業成長を加速させる基盤」と位置づけています。生成 AI の価値は、導入すること自体ではなく、企業の情報とガバナンスが守られた状態で、全社的に安心して使い続けられることにあります。SynX は、これまで培ってきたセキュリティ評価の知見を活かし、お客様が生成 AI の利活用とリスク管理を両立できる環境づくりを支援してまいります。

■ 今後の展開

今後は、「生成 AI セキュリティアセスメント」と「生成 AI ガバナンス・セキュリティ構築」の 2 サービスを中心に、サービスの標準化と実績の確立を進めます。そのうえで、将来的には以下の領域への展開を目指します。

- AX（AI トランスフォーメーション）支援伴走サービス
- AI アプリケーションのセキュリティ診断
- 生成 AI 関連セキュリティ製品の販売・導入支援
- 当社グループが進める生成 AI 利活用支援との連携

また、SynXでは現在、AI エージェントを活用した業務変革を支援する AX（AI トランスフォーメーション）支援サービスの準備を進めています。業務の整理から AI エージェントの実装、ガバナンス整備、現場への定着までを一貫して支援するもので、本サービスで整えた安全な生成 AI 利用環境を土台に、企業の AI 活用を「守り」と「攻め」の両面から支援してまいります。

詳細は、改めてお知らせします。

■ 株式会社 SynX について

SynX は、開発・QA・IT インフラ・セキュリティを統合したサービス「SynX One」を提供し、企業の DX 推進と事業成長を支援しています。サイバーセキュリティ分野では、Web アプリケーション診断、ネットワーク診断、クラウド診断、IoT ペネトレーションテストなど、お客様の環境や要件に応じたセキュリティサービスを提供しています。

■ 本件に関するお問い合わせ先

株式会社 SynX

広報担当

Email：public.relations_desk@synx.co.jp

SynX ホームページ：<https://www.synx.co.jp/>