



October 15, 2026

Company Name: Pole To Win Holdings, Inc.
Representative: President & CEO Teppei Tachibana
(Stock code: 3657, Tokyo Stock Exchange, Prime Market)
Contact Person: Director & CFO Joji Yamauchi
(Email : ir@ptw.inc)

Notice Regarding the Launch of a New Service by Our Consolidated Subsidiary
~Launch of the “Generative AI Utilization Security Support Service”
to Help Enterprises Use Generative AI Safely and Securely~

We are pleased to announce that SynX Inc. (Headquarters: Chiyoda-ku, Tokyo; Representative Director and CEO: Junichiro Nishi; hereinafter “SynX”), a consolidated subsidiary of our company, has launched the “Generative AI Utilization Security Support Service” (hereinafter the “New Service”) to support the safe and secure use of generative AI in enterprises.

Generative AI is rapidly becoming widespread as a business infrastructure that integrates with corporate data and business processes, and interest in AI agents that autonomously perform tasks is also growing. At the same time, establishing a governance framework to support safe utilization—including addressing the risk of information leaks, dealing with unauthorized use of generative AI by employees (“shadow AI”), managing access rights, and implementing countermeasures against AI-specific security risks—has become a critical management challenge.

SynX, which has cultivated expertise in security risk analysis and countermeasure support through its vulnerability assessment services, has launched this new service against this backdrop. The new service consists of two components: the “Generative AI Security Assessment,” which visualizes generative AI usage and associated risks, and the “Generative AI Governance and Security Implementation,” which supports the establishment of AI governance frameworks and information protection measures based on the assessment results. It provides comprehensive support for the formulation of AI usage guidelines, DLP, identity and access management, training, and incident response, enabling companies to balance AI adoption with risk management.

As the use of generative AI and AI agents expands within enterprises, demand for related security solutions is expected to grow. Starting with these services, SynX plans to strengthen its track record and service infrastructure, with the goal of expanding its business scope in the future to include security diagnostics for AI applications and AI Transformation (AX) support services. Our group will establish an integrated service delivery framework—ranging from the security domain that underpins AI adoption to business transformation support—to comprehensively support companies in their use of AI.

Our Group, which holds a top-tier market share in Japan for game QA, has identified the domestic tech sector—centered on non-game software testing—as one of our growth areas. While we believe the impact of this initiative on our business performance will be minimal at this time, we expect it to contribute to strengthening our revenue base in the medium to long term.

Please refer to the attached materials for details on the new service.

■SynX Launches “Generative AI Utilization Security Support Service” to Help Enterprises Use Generative AI Safely and Securely ~Leveraging expertise gained through vulnerability assessments to support the development of governance frameworks for the safe use of generative AI~

SynX Launches “Generative AI Utilization Security Support Service” to Help Enterprises Use Generative AI Safely and Securely ~ Leveraging expertise gained through vulnerability assessments to support the development of governance frameworks for the safe use of generative AI~

SynX Inc. (Representative Director and CEO: Junichiro Nishi; Headquarters: Chiyoda-ku, Tokyo; Major Shareholder: Pole To Win Holdings, Inc. (100%); listed on the Tokyo Stock Exchange Prime Market (Stock Code: 3657); hereinafter “SynX”) is pleased to announce the launch of its “Generative AI Utilization Security Support Service,” designed to assist companies in the safe use of generative AI.



Through this service, SynX is expanding its business into the generative AI security domain by leveraging the security assessment expertise it has cultivated through its security vulnerability assessments. Based on the philosophy of “security for the safe use of generative AI” rather than “security designed to prevent the use of generative AI,” SynX supports the creation of systems that balance the promotion of usage with risk management.

■ Background of the Launch of the Service

Generative AI is rapidly evolving from a tool for individual use into a core component of corporate operations. Beyond content creation and search assistance, organizations are increasingly integrating generative AI with corporate data and business processes for applications such as internal information retrieval, document preparation, development, customer support, Retrieval-Augmented Generation (RAG), and AI agents.

As a result, the key challenge surrounding generative AI is no longer whether enterprises should allow employees to use AI tools. Instead, it has become a matter of information governance and access control: determining what information can be accessed, by whom, through which AI systems, and to what extent. While the adoption of

generative AI continues to accelerate across enterprises, it also gives rise to a range of security and governance challenges, including the following:

- **The risk of information leaks** resulting from inputting confidential information, personal information, customer data, source code, and internal documents into AI systems
- “Shadow AI”—the use of generative AI tools, personal accounts, or unauthorized AI services in business operations without the company’s knowledge
- **The importance of designing access rights for source data**, as generative AI, when integrated with internal data, may search for and summarize information that users previously could not locate
- **Addressing AI-specific security risks**—such as prompt injection, disclosure of confidential information, excessive agency, RAG/vector-related issues, and the AI supply chain—**which differ from those of traditional web systems**

Moreover, even when the use of generative AI is prohibited, employees may still access external AI services, creating a phenomenon known as "Shadow AI," where companies are unable to monitor or control AI usage. In addition, the risks associated with generative AI are not limited to the responsibility of security teams alone. They affect multiple functions across the organization, including information systems, legal and compliance, data governance, human resources and training, as well as business units.

Therefore, companies must go beyond individual decisions—such as “banning ChatGPT” or “implementing Copilot”—and establish an “AI governance framework” that encompasses who will manage the systems, what services will be permitted, what data can be input, how new AI services will be evaluated, and how incidents will be handled.

The OWASP GenAI Security Project has systematized key security risks related to LLMs, generative AI, and AI agents, such as prompt injection, disclosure of confidential information, and excessive agency.

Additionally, NIST’s AI Risk Management Framework (AI RMF) outlines an organizational approach to AI risk management based on the principles of “Govern, Map, Measure, and Manage.” Against this backdrop, SynX is launching a security support service to enable the safe utilization of generative AI, leveraging the expertise gained through its existing security vulnerability assessments.

■ Overview of the “Generative AI Utilization Security Support Service”

This service consists of two components: “**the Generative AI Security Assessment,**” which visualizes a company’s generative AI usage and identifies security and governance challenges; and “**Generative AI Governance and Security Implementation,**” which provides support for concrete improvements to address the identified issues.

STEP 1: Generative AI Security Assessment

We assess a client company's generative AI usage to identify security and governance risks and areas for improvement. We evaluate generative AI usage, data handling practices, information leakage risks, ID and access rights, and usage policies and frameworks, and present a roadmap for improvement.

STEP 2: Generative AI Governance and Security Implementation

We provide concrete support to address the issues identified in STEP 1 and build an environment where generative AI can be utilized safely.

Key Support Services

- AI Usage Guidelines
- AI Governance Framework
- Information Protection and DLP
- ID and Access Management
- Training and Incident Response

■ Applying Insights Gained from Security Vulnerability Assessments to the Generative AI Domain

SynX has long provided security vulnerability assessment services targeting web, mobile, network, cloud, and IoT environments. With this new service, we are leveraging our accumulated security assessment expertise to expand our support scope into the generative AI security domain.

Building on traditional security assessments focused on “discovering vulnerabilities,” we provide step-by-step support for the security challenges companies face when utilizing generative AI—from assessments that visualize usage patterns and challenges to the establishment of governance and security frameworks.

For customers currently using our existing security vulnerability assessment services, we can also propose security support for generative AI adoption based on the system environments and challenges identified through those assessments.

Service Menu

Service	Price
Generative AI Security Assessment	From 1 million yen
Generative AI Governance and Security Implementation	From 2 million yen

*Prices vary depending on the scope and details of the project. Please contact us for more information.

■ Service Process

This service is provided following the process outlined below, starting with SynX's security vulnerability assessment.

① Assessment of Generative AI Usage

We will assess your generative AI usage, data handling practices, usage policies, and management framework.

② Visualizing Security and Governance Challenges

We identify security and governance risks associated with the use of generative AI, as well as areas for improvement.

③ Proposal of an Improvement Roadmap

Based on the assessment results, we will present priority issues and directions for improvement.

④ Establishing Governance and Security

As needed, we will assist in establishing AI usage guidelines, a governance framework, information protection and DLP measures, identity and access management, training, and incident response procedures.

Process for Providing Security Support Services for Generative AI Adoption (Steps 1–4)

■ SynX's Vision for Generative AI Security

SynX views generative AI not as a “risk that should be prohibited,” but as a “foundation for accelerating business growth through safe utilization.” The value of generative AI lies not in its adoption alone, but in the ability to continue using it with confidence across the entire organization while ensuring that corporate information and governance are protected. Leveraging the security assessment expertise we have cultivated over the years, SynX will support our clients in creating an environment where they can successfully balance the utilization of generative AI with effective risk management.

■ Future Plans

Moving forward, we will focus on standardizing our services and establishing a proven track record, centered on two core services: “Generative AI Security Assessment” and “Generative AI Governance and Security Implementation.” Building on this foundation, we aim to expand into the following areas in the future.

- AX (AI Transformation) Support and Guidance Services
- Security Diagnostics for AI Applications
- Sales and Implementation Support for Generative AI-Related Security Products
- Collaboration with our group's generative AI utilization support initiatives

Additionally, SynX is currently preparing an AX (AI Transformation) support service designed to assist with business transformation using AI agents. This service provides end-to-end support—from streamlining business processes to implementing AI agents, establishing governance frameworks, and ensuring adoption on the front lines. Building on the secure generative AI environment established through this service, we will support companies' AI adoption from both a “defensive” and “offensive” perspective.

Further details will be announced at a later date.

■ About SynX

SynX provides “SynX One,” an integrated service combining development, QA, IT infrastructure, and security services, to support companies in advancing digital transformation (DX) and driving business growth. In the cybersecurity field, we offer security services tailored to our clients' environments and requirements, including web application assessments, network assessments, cloud assessments, and IoT penetration testing.

■ Contact Information

SynX Inc. (Public Relations)

Email: public.relations_desk@synx.co.jp

SynX Website: <https://www.synx.co.jp/>