FOR IMMEDIATE RELEASE

CybExer and Cyber Defense Labs Support Keio University Global Research Institute in Assessing Cyber Resilience for Japan's Critical Infrastructure

— Reproducing and observing dynamic attacks within integrated OT/IT environments —

CybExer, an Estonian deep-tech cyber range company, is supporting Keio University Global Research Institute in Japan in establishing an OT/IT cyber resilience test environment. Using CybExer's world-class cyber range platform and digital twin capabilities, the environment replicates critical system architectures and enables the dynamic reproduction and observation of attack–defense interactions over time across repeatable attack scenarios—supporting resilience assessment under conditions that mirror real operations.

Keio University

CYBER DEFENSE LABS
サイバー防衛研究所

×

CybExer

Keio University Global Research Institute (Director: Teruo Nakatsuma; hereinafter KGRI) is advancing research and development of a Dynamic Penetration Testing platform to practically evaluate the resilience of OT/IT hybrid environments. This initiative is part of the New Energy and Industrial Technology Development Organization (NEDO)'s "Economic Security Critical Technology Development Program (hereinafter referred to as the K Program)/Enhancement of Advanced Cyber Defense Functions and Analytical Capabilities" (JPNP24003).

This research and development is being conducted with KGRI as the primary research entity. Cyber Defense Labs, K.K. (Headquarters: Shinjuku, Shinjuku-ku, Tokyo; President and CEO: Toru Tsuchiya) and CybExer (CybExer, CEO: Andrus Kivisaar) are providing technical support as external contractors involved in the development of this platform.

■ Background

Cyberattacks targeting critical infrastructure and industrial systems are becoming increasingly sophisticated and complex. Traditional static security assessments alone are insufficient to fully understand system resilience in real operational environments.

Particularly in environments integrating OT (Operational Technology) and IT (Information Technology), the interaction between attack and defense evolves over time, increasing the need for a dynamic verification platform aligned with operational realities.

The dynamic penetration testing referred to in this research is a methodology that continuously reproduces and observes the interaction between attack and defense over time within an environment simulating actual operation, thereby evaluating the system's resilience characteristics.

■ Research and Development Overview

This research builds a high-fidelity simulator combining real hardware environments with attack scenario technology, enabling the dynamic reproduction and observation of attack-defense interactions within OT/IT integrated environments.

Unlike conventional verification environments centered on static evaluation, the technical novelty lies in enabling continuous security verification under conditions simulating actual operation.

This platform aims to achieve the following:

・Reproduction of attack scenarios close to real environments
・Execution of dynamic attack scenarios tailored to OT/IT integrated environments
・Quantitative assessment of system resilience and recovery capability
・Cross-cutting utilization for research, education, and practical exercises

■ Establishing Resilience Evaluation Metrics

This research advances the development of an indicator system for quantitatively evaluating system resilience from the following perspectives, aiming to establish practical evaluation methods for critical infrastructure sectors:

・Recovery: Characteristics of recovery following a failure
・Withstanding: Ability to maintain functionality under attack

This will enable the establishment of reproducible, operationally oriented resilience assessment.

■ Alignment with International Standards

The research outcomes will be organized with an eye toward alignment with international security and resilience frameworks such as the IEC 62443 series and NIST SP 800-160, aiming to ensure international interoperability. Particular emphasis will be placed on applying this framework to resilience verification in OT/IT integrated environments.

■ Societal Significance and Future Development

This initiative will contribute to:

・Advancing practical verification methods in critical infrastructure sectors
・Systematization of dynamic penetration testing
・Strengthening practical human resource development environments
・Enhancing cyber defense capabilities through industry-government-academia collaboration

Moving forward, we will pursue phased deployment in critical infrastructure sectors such as power and manufacturing, with a view toward demonstration, guideline development, and social implementation.

■ Endorsement

【Keio University】

Professor Emeritus, Keio University / Senior Advanced Research Project Professor, Keio University, Jun Murai stated:

"Amid increasing cyber risks surrounding critical infrastructure, establishing a verification platform designed for real operational environments holds significant meaning for effectively advancing Japan's cybersecurity policy. Through this initiative, we will further deepen collaboration among industry, government, and academia, contributing to strengthening Japan's overall cyber defense capabilities and human resource base."

【CybExer】

Andrus Kivisaar, CEO of CybExer, stated:

"We find it highly meaningful to collaborate with Cyber Defense Labs and contribute technically to Keio University's pioneering efforts. We expect this support to contribute to the development of Japan's cybersecurity ecosystem."

【Cyber Defense Labs, K.K.】

Toru Tsuchiya, President and CEO of Cyber Defense Labs, K.K. stated:

"We are honored to support Keio University's research and development efforts from a technical perspective by leveraging our expertise. Through this initiative, we will contribute to advancing practical cyber exercise environments in Japan."

■ Acknowledgments

This achievement is based on results obtained from a project, JPNP24003, commissioned by the New Energy and Industrial Technology Development Organization (NEDO).

【 About Keio University Global Research Instituite 】

The Keio University Global Research Institute (KGRI) was established in November 2016 as a research organization to bridge faculties and graduate schools across the university. KGRI aims to promote interdisciplinary and international collaborative research that goes beyond the boundaries of singular academic disciplines and international borders. It also aims to share research outcomes both in Japan and worldwide, further promoting engagement in joint research.

To achieve this goal, KGRI has set up more than 40 centers and projects funded by external sources or through internal grants, covering a wide range of research topics--from basic research to addressing social challenges facing the world.

URL : https://www.kgri.keio.ac.jp/en/about/index.html

【 About CybExer 】

CybExer specializes in defending digital ecosystems against growing cyber threats by providing cybersecurity and cyber range services. Through its suite of services based on digital twin technology, CybExer helps governments and critical infrastructure organizations proactively address cyberattacks.

URL: https://cybexer.com/

【 About Cyber Defense Labs, K.K. 】

Since its establishment in 2024, Cyber Defense Labs has pursued the mission of researching effective countermeasures against attackers' tactics and techniques in cyberspace, sharing information with like-minded organizations and groups, enhancing national security, realizing public-private cyber collaboration domestically and internationally, and becoming a leading research hub for cyber defense.

URL: https://cdlabs.jp/

【 Media Contact for This Release 】

Cyber Defense Labs. Public Relations
Mail: press@cdlabs.jp