

The 16th International Cybersecurity Symposium

“Cybersecurity for Digitized National Security, Economic Security, and Societal Security: Global Multilateral Public-Private Partnership Actions with Advanced Technologies such as AI and Quantum”

**Hosted by Keio University KGRI project CCRC/CSRC,
INCS-CoE, The MITRE Corporation, Sasakawa Peace Foundation
October 27 (Tue), 28 (Wed), 29 (Thu) & 30 (Fri), 2026, 9:00–18:00 JST (In-person)
Keio University, Mita Campus, Tokyo, Japan**

(Notes: The registration will be open around September inviting through e-mail)

Version 4

We invite you to join us for the 16th International Cybersecurity Symposium at Keio University's Mita Campus in Tokyo, organized by the Cyber Civilization Research Center (CCRC) and the Cyber Security Research Center (CSRC), both part of the Keio University Global Research Institute (KGRI). The main purpose is to continue our cross-cutting cybersecurity discussions with National Security, Economic Security, and Social Security. Some discussion themes include how to address negative use of cyber and Generative and Agentic AI, human civilization on our planet, geopolitical conflicts, ransomware impacts, Quantum technologies, Outer Space, and the digital technologies in our daily lives. The discussions will lead to the specific actions towards globally trusted multilateral Public-Private Partnerships, addressing the gaps and alliances in cybersecurity among countries, regions, G7, and G20.

In the National Security domain, we observe the hybrid attacks with cyber and physical with AI technologies having geopolitical tensions continuously. Multiple bilateral and multilateral organizations, such as Five Eyes, AUKUS, Quad, and NATO, are addressing the National Security concerns. In the meantime, Japan is preparing the plans to strengthen the structure with National Information Security agency after summer 2026 and plan to enact “Cyber Response Capability Strengthening Act and Necessary Arrangement of Relevant Acts” in October this year.

In the Economic Security domain, the critical infrastructure operators are expected to be trusted players with safe and secure in the social infrastructure. The global supply chain with evolutionary technologies, new development, procurement, and production by using AI and other innovative technologies are important core functions for national existence.

In the Societal Security domain, International Mutual Recognition is important to accomplish the Data Free Flow with Trust 2.0 (DFFT 2.0), while the OECD's Institute Agreement for Partnership (IAP) has been working supported by the G7 and G20. Further, the Personal Information Protection laws by country and region are significant for privacy of citizens and major decision-makers. It is important to balance between Data Use and Data Protection.

We invite the speakers and panelists from government, industry, and academia:

- Japanese Minister level, Ministries, and Agencies
- Ambassador level and each Embassy: U.S., UK, EU, Australia, Canada, France, Germany, Italy, Netherlands, Portugal, Estonia, Lithuania, Ireland
- United Nations, Keidanren, major corporations, former and current National Security executives

Supporters (in progress): Japanese government Ministries and Agencies, Embassies in Japan, NGOs, corporations, academia, etc.

Online registration and Program website: URL: <https://symp.cysec-lab.keio.ac.jp/2026oct/>

Draft Structure (Plan)

Day 1: Opening Day Highlights:

- Japanese Government Ministerial Remarks
- Remarks from each of the governments and United Nations
- Speeches from Japanese Government from Ministries and Agents
- Keynote Speeches

Day 2: National Security Highlights:

- Theme: PQC, International Emerging Technologies
 - Discuss on international policy, standardization, guidelines, and rulemaking for Post-Quantum Cryptography (PQC), Quantum technologies, AI-Quantum NEXUS, and other emerging technologies, including national security, economic security, technological competitiveness, trust, and international cooperation.
- Theme: Intelligence, National Intelligence Agency
 - Discuss on cyber threat intelligence sharing, strengthening national intelligence capabilities, and public-private partnership, including institutional frameworks and operational practices among governments, critical infrastructure operators, and private-sector organizations.
- Theme: National Security
 - (Presented by Sasakawa Peace Foundation)
- Theme: Active Cyber Defence, Utilization of SBOM
 - Discuss on institutional frameworks, operational structures, and intelligence coordination for Active Cyber Defence, including situational awareness, attribution, law enforcement, defense, intelligence cooperation, and strengthening national cyber response capabilities.
- Theme: Sovereign Cloud
 - Discuss on trusted digital infrastructure including national cloud, government cloud, including trusted cloud infrastructure and international collaborations considering cloud sovereignty, data protection, critical infrastructure, defense, and commercial cloud providers.

Day 3: Economic Security Highlights:

- Theme: Enhancing Technology, PETs
 - Discuss on Privacy-Enhancing Technologies (PETs), confidential computing, cryptographic technologies, and data clean rooms, including governance frameworks, trusted data utilization, and international interoperability.
- Theme: AI
 - Discuss on the impacts of Generative AI and Agentic AI on economic security, supply chains, critical infrastructure, and research and development, including AI safety, trustworthiness, governance, international standards, and international cooperation.
- Theme: Economic Security
 - (Presented by Sasakawa Peace Foundation)
- Theme: Critical Infrastructure, i.e. Energy
 - Discuss on cybersecurity and supply chain resilience in the electric power and energy sectors, including resilience enhancement and public-private partnership.
- Theme: Critical Infrastructure, i.e. Semiconductor
 - Discuss on the semiconductor supply chain, including design, manufacturing, equipment, materials, advanced packaging, diving into manufacturing site cybersecurity, intellectual property protection, and international cooperation.

Day 4: Societal Security Highlights:

- Theme: The Significance of Individual “Consent” in the Age of AI

- Discuss on legal frameworks centered on the Data Utilization Act and the Personal Information Protection Act, including policy design to balance data utilization and privacy protection, and international interoperability.
- Theme: Digital Nippon, Priority Plan for Realizing a Digital Society
 - Discuss on the Priority Plan for Realizing a Digital Society and the Digital Nippon initiative, including policy priorities, digital government, My Number, government cloud, AI, data utilization, and implementation challenges for integrating security and trust.
- Theme: Digital Trust Infrastructure
 - Discuss on practical implementation of data spaces supporting Digital Trust Infrastructure, including Battery Passports, CBAM, finance, healthcare, cross-industry data sharing, interoperability, and trusted digital ecosystems.
- Theme: Public Trust, ISO (Trusted List)
 - Discuss on institutional frameworks and international standards supporting digital signatures, digital certificates, and trust services, including Trusted Lists, accreditation schemes, auditing, ISO standards, and cross-border interoperability.
- Theme: Digital Identity Wallet, Electronic Attestation of Attributes
 - Discuss on policies, technologies, and implementation of Digital Identity Wallets and Electronic Attestation of Attributes (EAA), including trusted digital identity infrastructure, government services, private-sector applications, and cross-border data exchange.