PKI Progress in Japan
From July 2026 to October 2026

November 13, 2026

Atsushi INABA

Table of contents

1. Government related Updates

1.1 International perspective

(1) Digital Agency / OECD

- Vice Minister of Digital Agency attended the OECD DFFT Community of Experts and Senior Officials Meeting

1.2 Domestic perspective

(1) Digital Agency

- Published “the Priority Plan for the Advancement of a Digital Society” on July 21

Table of contents

2. Updates in the Private Sector

2.1 International perspective

(1) Proposal to ISO : International Trusted List

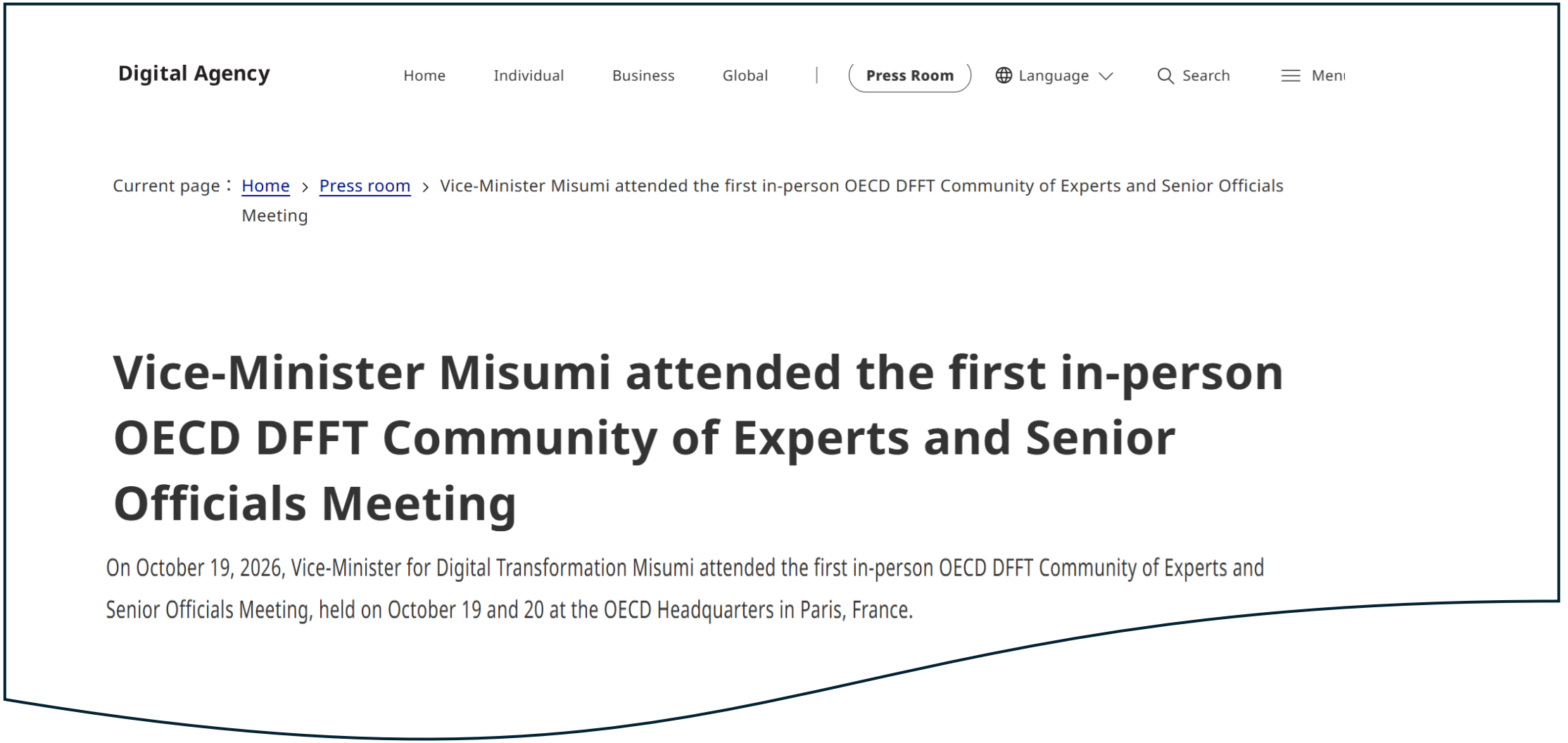
- By Keio University Team

2.2 Domestic perspective

(1) 16th International Cybersecurity Symposium

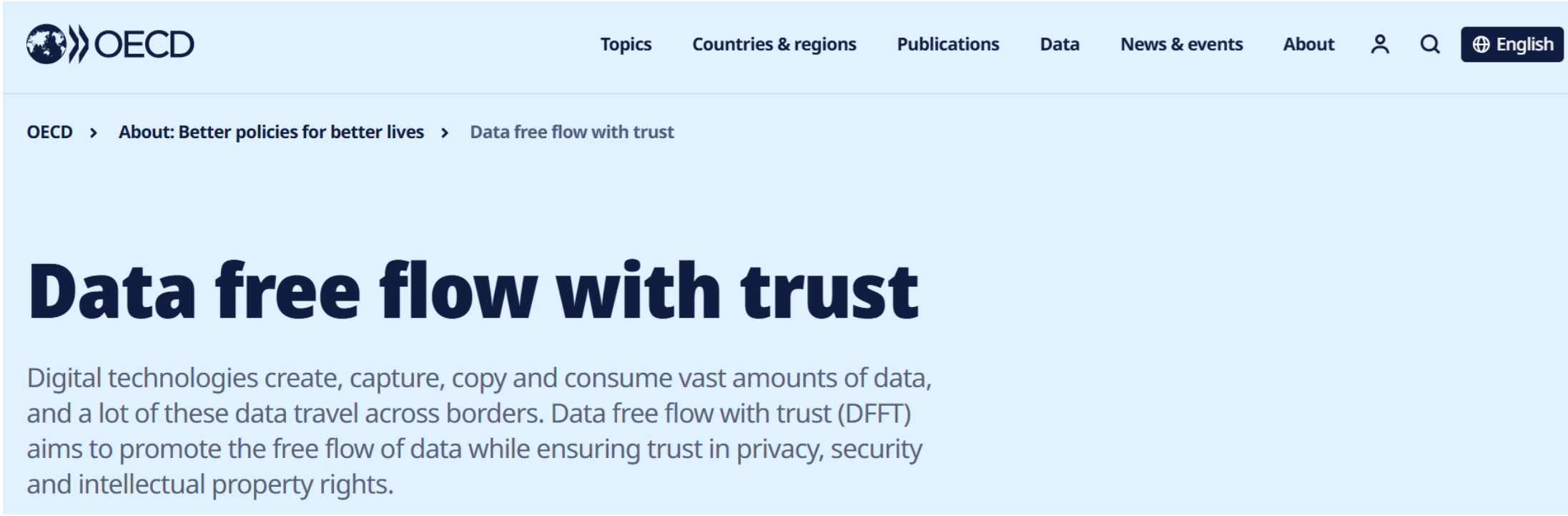
- Held in Tokyo from October 27 to October 30

Digital Agency / OECD



Cited from ： https://www.digital.go.jp/en/press/664c482f-3164-48d2-a3ee-5f1cf415cd78

OECD



Cited from： https://www.oecd.org/en/about/programmes/data-free-flow-with-trust.html

OECD

Latest news

OECD DFFT Community of Experts and Senior Officials Meeting

Trusted Data Flows Through Many Lenses: Expert Insights for Policy Actions

19-20 October 2026 (participation by invitation only)

This 3rd Plenary of the OECD DFFT Expert Community will bring together expert community participants and senior officials, delegates, leading experts and institutional partners to advance the Data Free Flow with Trust (DFFT) agenda. As cross-border data drives innovation and AI development, governments also seek to protect privacy, security and intellectual property — increasingly inspired by considerations of digital sovereignty, economic security and resilience. Reconciling these objectives is at the heart of building trust in cross-border data flows. The Plenary will:

- **Connect policy and practice:** exchanging insights from across the Community's working groups on how trust can be operationalised for cross-border data flows.
- **Showcase major outputs** including a live demonstration of the forthcoming OECD Privacy-Enhancing Technologies (PETs) Repository, the launch of new publications, and new OECD work on measuring cross-border data flows and trust.
- **Shape the DFFT agenda for 2027:** assessing emerging challenges, including the intersection of DFFT with economic security and resilience, and identifying priorities for future work.

Cited from ： https://www.oecd.org/en/about/programmes/data-free-flow-with-trust.html

OECD

Why the OECD?

The DFFT Expert Community is governed by the OECD Digital Policy Committee (DPC) through its Working Party on Data Governance and Privacy, drawing on experts nominated by Member countries and the Secretariat from government, academia, business, civil society and regulatory bodies.

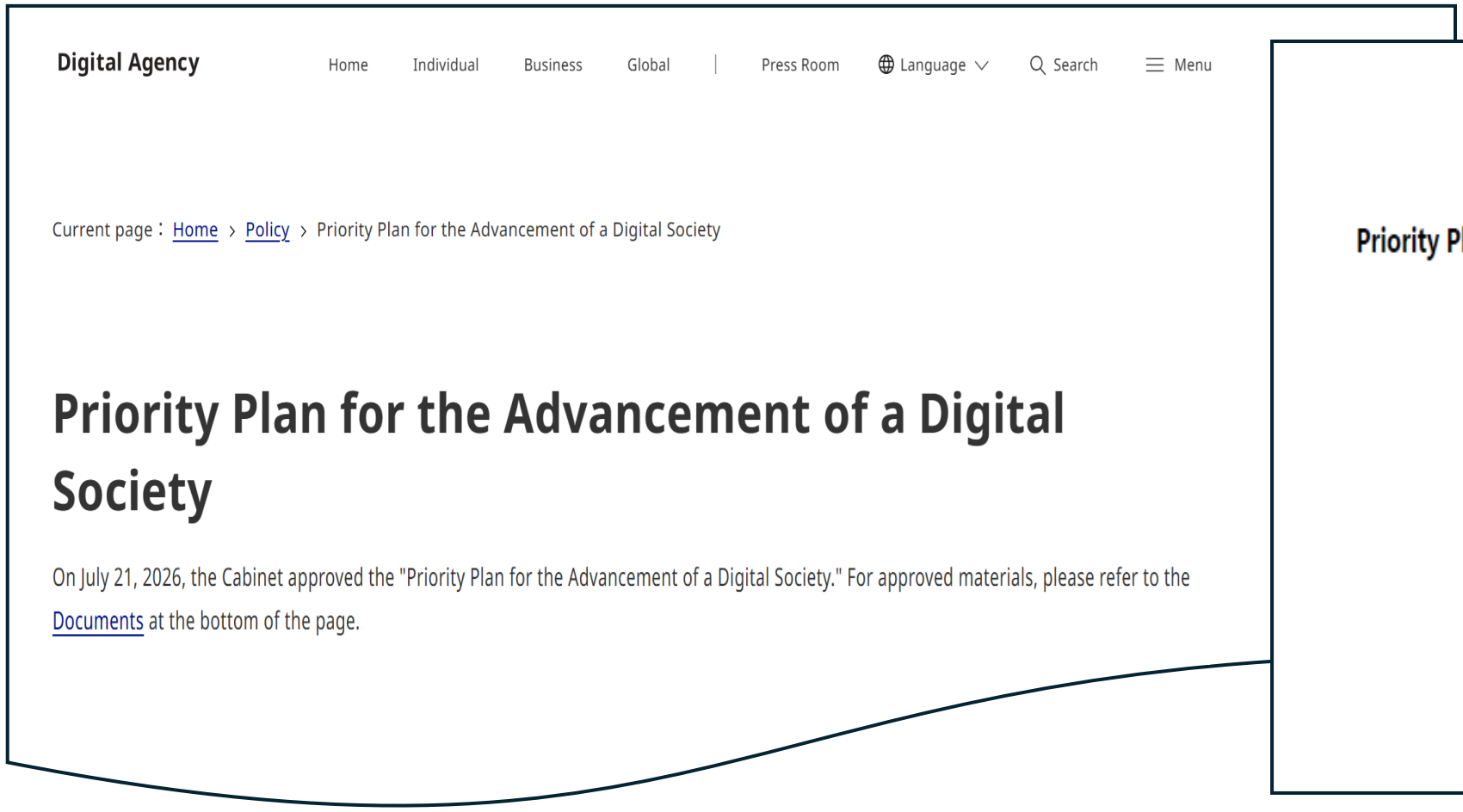
At the 2023 Hiroshima Summit, G7 Leaders endorsed the Institutional Arrangement for Partnership (IAP), combining intergovernmental decision-making with multi-stakeholder expertise and flexible cross-organisational partnerships. This commitment was operationalised under the OECD in December 2023, leveraging the Organisation's established expertise in digital policy, data governance, and privacy.

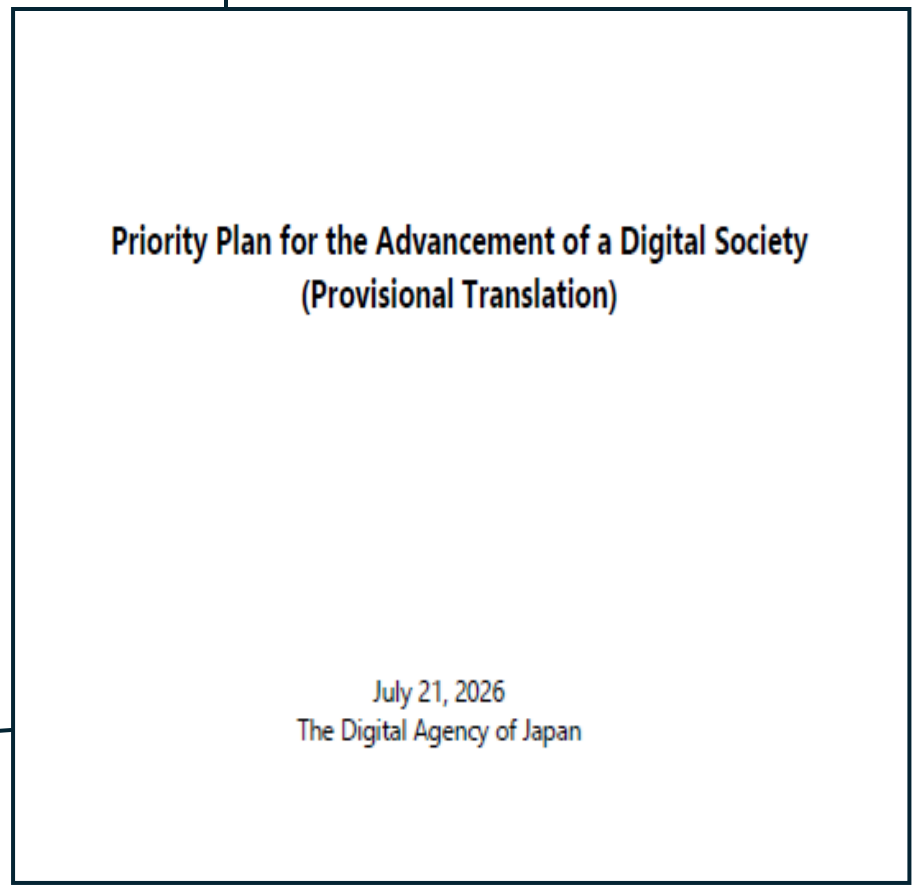
The OECD provides neutral, evidence-based analysis and a legitimate, inclusive space on data policy and governance involving cross-border data flows. The DFFT Community contributes to the policy outcomes of the OECD.

The work builds on OECD legal instruments that establish shared norms across the dimensions of trust, including the Recommendation on Enhancing Access to and Sharing of Data and complementary instruments on privacy, government access, AI, health data, and digital security.

Cited from ： https://www.oecd.org/en/about/programmes/data-free-flow-with-trust.html

Digital Agency





Cited from ： https://www.digital.go.jp/en/policies/priority-policy-program

Digital Agency / Priority Plan for Advancement of a Digital Society

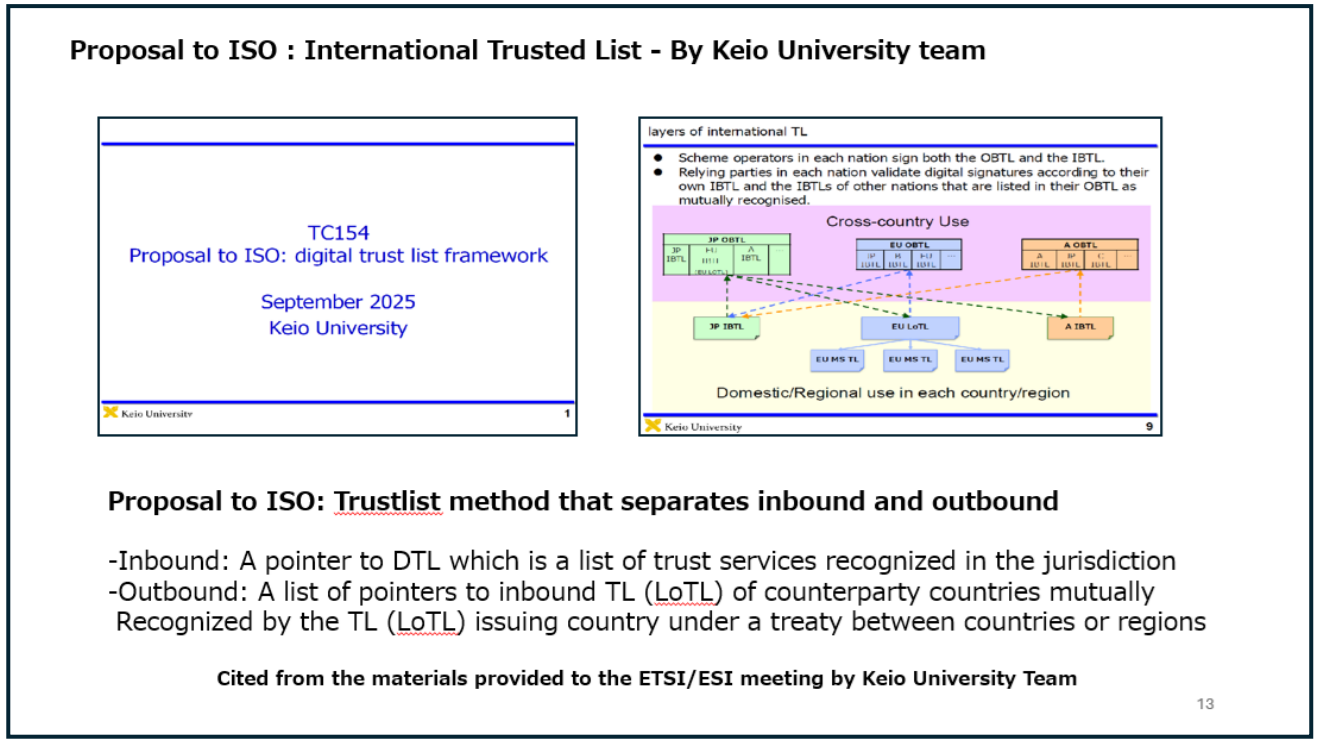
④ Improve the Security and Reliability of Government Information Systems, starting with the Government Public Key Infrastructure

(a) Smooth Migration to PQC

- As quantum computing technologies advance, there is growing concern that the security of public-key cryptography, which is currently widely used, may decline or be compromised. In this context, we aim to complete the migration to PQC at government agencies and other bodies by 2035 in principle. To this end, while considering how cryptographic technologies are used at government agencies and other bodies, we will work with the relevant ministries and agencies to develop a roadmap in FY2026 and, based on it, promote smooth migration to PQC.
- In addition, to promote migration to PQC across industries, we will develop guidelines and other materials that include specific procedures for conducting a crypto inventory (an inventory of the cryptography applied to information and systems held by a company).

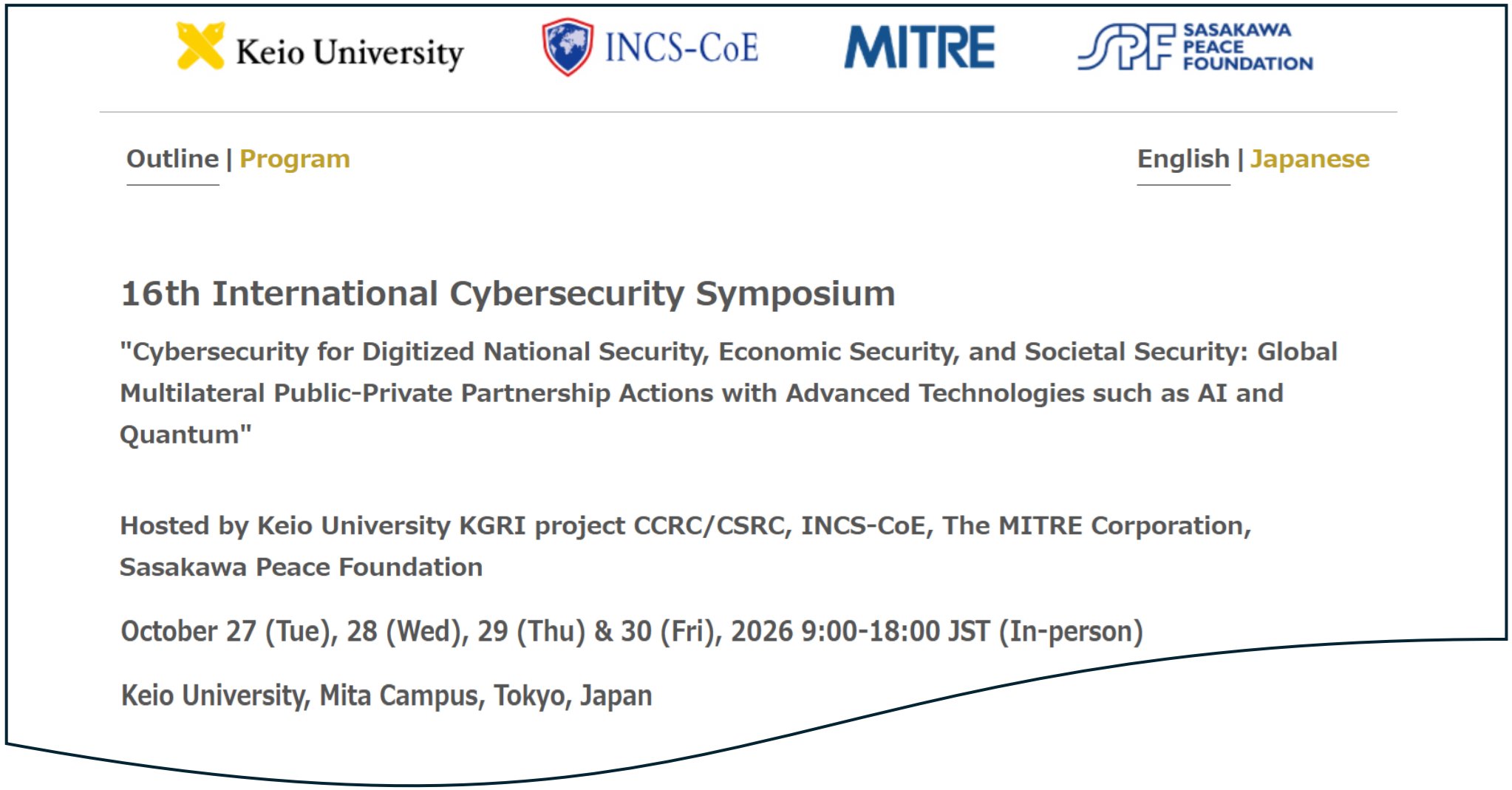
Cited from ： https://www.digital.go.jp/assets/contents/en/node/basic_page/field_ref_resources/5ecac8cc-50f1-4168-b989-2bcaabffe870/7a7ae67c/20260831_policies_priority_outline_en_02.pdf

Proposal to ISO : International Trusted List - By Keio University team



-The progress of the Keio University team's efforts toward ISO standardization reported several times at the ETSI related events and meetings this year. Furthermore, it was reported at the International Cybersecurity Symposium held in Japan from October 27 to October 30.
-The team has been working with the EU and India to achieve international mutual recognition of trust services, and it will be expected to expanding this kind of co-work with Asian countries in the future.

International Cybersecurity Symposium



Cited from ： https://symp.cysec-lab.keio.ac.jp/2026oct/index.html

International Cybersecurity Symposium

Purpose of the Event

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 central purpose of this 16th edition is to continue our cross-cutting cybersecurity discussions integrating National Security, Economic Security, and Societal Security. We have just released the draft program and the initial lineup of distinguished global leaders who will join us in Tokyo.

In the National Security domain, our current global landscape faces continuous cyber-physical hybrid attacks driven by highly advanced AI, occurring against a backdrop of ongoing geopolitical tensions. Multilateral coalitions such as the Five Eyes, AUKUS, Quad, and NATO are actively addressing these security threats. Meanwhile, Japan is rapidly solidifying its defense posture, preparing to establish its National Information Security Agency after summer 2026, and aiming to enact the "Cyber Response Capability Strengthening Act and Necessary Arrangement of Relevant Acts" in October this year.

In the Economic Security domain, operators of critical infrastructure must act as secure and trusted players. Securing global supply chains including procurement, production, and R&D facilitated by innovative AI is critical for national resilience. This demands robust public-private partnerships, national cybersecurity strategies, and security clearance frameworks.

In the Societal Security domain, achieving Data Free Flow with Trust 2.0 (DFFT 2.0) relies heavily on international mutual recognition, supported by the OECD's Institute Agreement for Partnership (IAP) endorsed by G7 and G20. Furthermore, balancing data utilization with citizens' privacy protection through domestic and regional personal information protection laws remains essential.

Addressing these global dynamics, this year's symposium brings together top-tier speakers from government, industry, and academia to discuss the negative uses of cyber and generative/agentic AI, the future of human civilization, geopolitical conflicts, ransomware, quantum technologies, outer space, and digital technologies in our daily lives. The ultimate goal is to formulate actionable steps toward trusted, globally aligned, multilateral Public-Private Partnerships that bridge international gaps and foster stronger alliances across regions, the G7, and the G20.

Cited from ： https://symp.cysec-lab.keio.ac.jp/2026oct/index.html

International Cybersecurity Symposium

【Draft Program Outline】

■ Day 1: Opening Day Highlights
* Japanese Government Ministerial Remarks
* Remarks and greetings from international governments and the United Nations
* Speeches from Japanese Government Ministries and Agencies
* Keynote Speeches

■ Day 2: National Security Highlights
* Theme
  ・PQC, International Emerging Technologies
  ・Intelligence, National Intelligence Agency
  ・National Security (Presented by Sasakawa Peace Foundation)
  ・Active Cyber Defence
  ・Sovereign Cloud

■ Day 3: Economic Security Highlights
* Theme
  ・Enhancing Technology, PETs
  ・AI
  ・Economic Security (Presented by Sasakawa Peace Foundation)
  ・Critical Infrastructure, i.e. Energy
  ・Critical Infrastructure, i.e. Semiconductor

■ Day 4: Societal Security Highlights
* Theme
  ・The Data Utilization Act and the Amended Personal Information Protection Act
  ・Digital Nippon, Priority Plan for Realizing a Digital Society
  ・Digital Trust Infrastructure
  ・Public Trust, ISO (Trusted List)
  ・Digital Identity Wallet, Electronic Attestation of Attributes

Cited from ： https://symp.cysec-lab.keio.ac.jp/2026oct/index.html

Thank you