Cybersecurity 2026 (FY2025 Annual Report / FY2026 Annual Plan)

Trends in Cyber Threats and Responses

- As Japan faces its most severe and complex security environment since the end of World War II, **the environment surrounding cyberspace has become increasingly serious in recent years.**
- **The social impact of damage caused by cyber attacks through supply chains, etc., remains significant.**
- **We face new threats due to the rapid advancement of AI.**

- Promote the **development of the Cyber Response Capability Strengthening Act and Necessary Arrangement of Relevant Acts** (the Strengthening Act, etc.), the formulation of a new **Cybersecurity Strategy**, **the improvement of measures and resilience at government agencies and related agencies and critical infrastructure**, and the **strengthening of international cooperation**.

Main Implementation Results and Evaluation of Cybersecurity-Related Measures in FY2025

- Measures set out in the previous year's annual plan and the new strategy have progressed steadily as planned.
- Meanwhile, coupled with the advancement of AI, it is necessary to strengthen related measures further and respond in an agile manner while taking into account changing circumstances, including AI.

Two Measures Positioned as "Measures that Require Particularly Strong Commitment" in FY2026

Cybersecurity as one of the cross-sectoral issues in Japan's Growth Strategy

- **To underpin investments that promote growth in the 17 strategic fields, we will strengthen our response to cyber threats based on the "Cybersecurity Strategy"** through the steady implementation of the Strengthening Act, etc., as well as the flexible review of related systems.

(i) Improving cybersecurity and resilience across society

(ii) Defense and deterrence against cyber threats promoted with the government playing pivotal roles

(iii) Fostering and securing human resources, technology, and industry to strengthen Japan's cyber response capabilities and ensure autonomy

(IV) Responding to technological advances in AI and other fields

Project "YATA-Shield"

Protecting CI and Gov. agencies

- **Alerts and Guidance** for
  - **Critical Infrastructure Operators**
  - **Government Agencies**
- **Public-Private Partnership mechanism** from the Financial Sector to All Sectors
- Support for **Cyber Workforce** Development (i.e. NICT, IPA etc.)

Enhancing Vulnerability Detection and Patch Management

- **Alerts and Guidance for Software Vendors**
- Enhancing further collaboration with **International Partners, AI Developers**
- **AI Safety Institute (AISI)**'s Technical Support and Assessment
- **Promotion of R&D** on AI Security Technologies
- **NCO-led** Enhancement of **Cyber Response Capabilities using Advanced AI**

Measures that Require Particularly Strong Commitment (1) Cybersecurity as one of the cross-sectoral issues in Japan's Growth Strategy

- In November 2025, the Headquarters for Japan's Growth Strategy, established within the Cabinet, identified cybersecurity as one of the eight cross-sectoral issues, and discussion and examinations were conducted at the Cybersecurity Promotion Expert Committee.
- The response to cybersecurity as one of the cross-sectoral issues in Japan's Growth Strategy has been positioned as one of the "Measures that Require Particularly Strong Commitment" for FY2026.

■ Policy direction (Summary)

To underpin investments that promote growth in the 17 strategic fields, we will strengthen our response to cyber threats based on the "Cybersecurity Strategy" through the steady implementation of Cyber Response Capability Strengthening Act and Necessary Arrangement of Relevant Acts, as well as the flexible review of related systems. In doing so, we will examine approaches to ensuring sustainable cybersecurity through public-private cooperation, based on a shared understanding that these measures constitute essential investments for growth.

■ Package of initiatives to be implemented (Summary)

① Improving cybersecurity and resilience across society

・**Strengthening measures across the entire supply chain, starting with the 17 strategic fields,** through initiatives such as the development of the "Supply Chain Security Evaluation System" (SCS Evaluation System). **Strengthening measures in the critical infrastructure sector,** through initiatives such as the formulation of the "Common Cybersecurity Standards for Critical Infrastructure". **Strengthening measures at government agencies and related agencies,** through initiatives such as the building and operating resilient information systems and urgent examination to proceed with the deployment of The High- Confidential Sovereign Cloud (tentative name). **Raising the standard in areas requiring further measures**, such as local governments, small and medium-sized enterprises (SMEs), the medical sector, and universities.

② Defense and deterrence against cyber threats promoted with the government playing pivotal roles

・Treating measures on the defensive side and measures to counter attackers as "two sides of a coin," with initiatives based on Cyber Response Capability Strengthening Act and Necessary Arrangement of Relevant Acts, **the government will play a pivotal role in promoting the defense and deterrence against cyber threats across the entire public and private sectors** by continuously imposing costs on attackers on an ongoing basis.

③ Fostering and securing human resources, technology, and industry to strengthen Japan's cyber response capabilities and ensure autonomy

・Promoting the use of cybersecurity workforce framework. Providing education and training opportunities to enhance the skills of security personnel at companies and other organizations, improving the capabilities of young engineers, and strengthen cybersecurity education at universities and other institutions.
・Promoting domestic cybersecurity technology, R&D, and industrial development, through initiatives such as promoting cybersecurity R&D programs, and the active utilization and evaluation advanced and promising security products and services within government agencies, including coordination with initiatives based on the "Public-Private Investment Roadmap" for various products and technologies.

④ Responding to technological advances in AI and other fields

・**Prompt implementation of necessary measures, based on Project "YATA-Shield", such as vulnerability assessments of critical government-wide systems by using AI.** Consolidating cybersecurity-related information, and examining and refining approaches to utilizing AI when handling highly confidential data. Fundamentally strengthening AISI's capabilities. Strengthening of public-private collaboration on AI security by enhancing initiatives such as information sharing in coordination with IPA and AISI, under the framework of the new council.
・Formulating a roadmap for the transition to post-quantum cryptography (PQC) in government agencies and related agencies, developing guidelines to support the transition in the industry sector and conducting demonstrations to assist with the transition process. Developing guidelines for deployment and operation that take into account Quantum Key Distribution's characteristics and by conducting demonstrations to address technical challenges.

Measures that Require Particularly Strong Commitment (2): Project "YATA-Shield"

- AI technologies are advancing and proliferating rapidly, and with AI being used maliciously in cyberattacks, the speed and scale of attacks are dramatically increasing, creating a situation where we face threats in cybersecurity.
- In May 2026, following the Prime Minister's instruction, Cybersecurity Minister Matsumoto compiled Action Package reflecting the increasing speed and scale of AI-enabled cyberattacks. Based on this package, relevant ministries, agencies, and other organizations will implement these measures promptly and accurately.
- In light of this, Project "YATA-Shield" is positioned as a "Measures that Require Particularly Strong Commitment" in FY2026.

Project "YATA-Shield" (May 2026)

On May 18, following the **Prime Minister's instruction**, **Cybersecurity Minister Matsumoto** compiled **Action Package** reflecting the increasing **speed and scale of AI-enabled cyberattacks**.

Protecting CI and Gov. agencies

- **Alerts and Guidance** for
  - **Critical Infrastructure Operators**
  - **Government Agencies**

  Calling for: **management class leadership**
  fundamental cybersecurity measures
  vulnerability management
- **Public-Private Partnership mechanism** from the Financial Sector to All Sectors
- Support for **Cyber Workforce** Development (i.e. NICT, IPA etc.)

Enhancing Vulnerability Detection and Patch Management

- **Alerts and Guidance for Software Vendors**
- Enhancing further collaboration with **International Partners, AI Developers**
- **AI Safety Institute (AISI)**'s Technical Support and Assessment
- **Promotion of R&D** on AI Security Technologies
- **NCO-led** Enhancement of **Cyber Response Capabilities using Advanced AI**

*YATA-Shield: "YATA" refers to the Yata-no-Kagami, a sacred mirror in Japanese mythology that illuminates the truth. Based on this concept, Project YATA-Shield aims to accurately understand the threats posed by advanced AI and promote cybersecurity measures to defend whole of society.