Press Release

An Announcement on co-sealing of the international guidance “Mitigating Cyberthreats with Limited Resources: Guidance for Civil Society”

May 15, 2024
The National Center of Incident Readiness and Strategy for Cybersecurity (NISC)
The National Police Agency

1. Overview

On May 15 the NISC and the National Police Agency jointly co-sealed international guidance for “Mitigating Cyberthreats with Limited Resources: Guidance for Civil Society” (hereinafter referred to as “this guidance”), which is led by the U.S. Cybersecurity and Infrastructure Security Agency (CISA), and are publicizing this guidance.

In addition to U.S. and Japan, Canada, Estonia, Finland, and the United Kingdom co-sealed this guidance and listed their authorities as authoring agencies in this guidance. On May 14 the Strategic Dialogue on Cybersecurity of Civil Society under Threat of Transnational Repression, of which the above countries are members, was held in Birmingham in the UK, and at the same time, this guidance was released.

In Japan, it has been confirmed that academics, think tanks, journalists, etc., which are referred to in this guidance, are targets of cyberattacks. Given the importance of this guidance, which shows risk mitigation measures to be taken by civil society, Japan has decided to co-seal it.

We will continue to strengthen international cooperation in the field of cybersecurity.

2. The abstract of this guidance

This guidance states that “civil society”, regarded as a set of organizations and individuals involved in the defending human rights and advancing democracy, is at high risk of becoming a victim of cyberattacks by state-sponsored threat actors aiming to undermine the democratic values, and it lists risk mitigation measures that should be taken.

(1) Subjects

Organizations and individuals involved in the protection of human rights and the promotion of democracy, such as academics, think tanks, journalists, and NGOs

(2) Threats

This guidance states that according to industry reporting, the state-sponsored actors targeting high-risk communities predominantly emanate from the governments of Russia, China, Iran, and North Korea. In the annexes, the names of groups and the specific tactics, techniques, and procedures (TTPs) of their attacks are described.

(3) Mitigations

(a) This guidance lists, and it recommends risk mitigations for organizations and individuals subjected to attacks, such as enabling multi-factor authentication (MFA), using proper account management, limiting exposure of personal information, encryption, using trusted app stores, and regular rebooting devices to eliminate spyware.

(b) This guidance also recommends that software manufacturers actively implement the Secure by Design Pledge and take responsibility for customer security outcomes.

3. Related link

CISA Resources site (Mitigating-Cyber-Threats-Limited-Resources-Guidance-Civil-Society)

4. Contact information

The National Center of Incident Readiness and Strategy for Cybersecurity
International Strategy Group
Councilor Mr.Yamaguchi, Mr.Kanai
Phone: +81-3-3580-3188