NISC National center of Incident readiness and Strategy for Cybersecurity

MEMTEC MIDDLE EAST MILITARY TECHNOLOGY CONFERENCE

National Cybersecurity Framework of Japan

29th October 2019

Hidetoshi OGAWA
Counsellor/Director of International Strategy
NISC, Cabinet Secretariat

Cybersecurity Strategic Headquarters

Cabinet

Prime Minister

IT Strategic Headquarters

Cooperation

Cybersecurity Strategic Headquarters

Established in accordance with the Basic Act on Cybersecurity, 9 January, 2015

Chair: Chief Cabinet Secretary

Deputy Chair: Minister of State in charge of functions related to the Cybersecurity Strategic Headquarters

Members:
- Chairman of the National Public Safety Commission
- Minister for Internal Affairs and Communications
- Minister for Foreign Affairs
- Minister of Economy, Trade and Industry
- Minister of Defense
- Minister in charge of Information Technology Policy
- Minister in charge of the Tokyo ...mpic and Paralympic Games
- Experts

Cooperation

National Security Council（NSC）

Cooperation

Cybersecurity Council

(Secretariat)

National Center of Incident Readiness and Strategy for Cybersecurity (NISC)

Established by Cabinet Order, 9 January, 2015

Director-General

Deputy Director-General

Cybersecurity Assistant

- Government Security Operation Coordination team（GSOC）
- Cyber Incident Mobile Assistant Team **(CYMAT)**

Competent Ministries of Critical Infras.

- Financial Services Agency 【bank, security, insurance】
- Ministry of Internal Affairs and Communications 【local governments, information and comm.】
- Ministry of Health, Labour and Welfare 【medical service, water supply】
- Ministry of Economy, Trade and Industry 【electricity, gas, chemistry, credit card, petroleum 】
- Ministry of Land, Infra, Transport and Tourism 【railway, aviation, logistics, airport】

Cooperation

Cooperation

Ministries under HQ Members

- National Police Agency
- Ministry of Internal Affairs and Communications
- Ministry of Foreign Affairs
- Ministry of Economy, Trade and Industry
- Ministry of Defense

Critical infrastructure operators, etc.

Government organizations

Companies

Individuals

Japan's Cybersecurity Framework and NISC

- The **Basic Act on Cybersecurity** provides:
  - Definition of "Cybersecurity" in legal context
  - Position of Cybersecurity Strategy
  - Authority and mandate of **Cybersecurity Strategic HQ**, which consists of Ministers and notable experts
- As the secretariat of Cybersecurity HQ, **NISC** (Cabinet Secretariat) works under the HQ's mandate, mainly as:

① National coordinator & Baseline setter of Cybersecurity - integrating and advancing cybersecurity policies crossing over governmental bodies

  - Cybersecurity Strategy
  - Cybersecurity Policy for Critical Infrastructure Protection
  - Common Standard on Information Security Measures of Government Entities
  - Cybersecurity Human Resource Development Plan
  - Cybersecurity Research and Development Strategy etc.

② Operational body as governmental CSIRT - monitoring, analyzing, and handling cyber attacks to governmental bodies on 24/7 basis, as well as assisting them in case of severe cyber incidents by sending a special assistance team "CYMAT".

Outline of the Cybersecurity Strategy 2018 (tentative translation)

Goals, Principles, Philosophy, and Approaches

- Develop Free, fair and secure cyberspace, subsequently contribute to 1) Socio-economic Vitalization and Sustainable Development, 2) Safe and Secure Society, and 3) International Peace & Stability and Nat'l Security;
- Based on principles of 1）Free Flow of Information, 2) Rule of Law, 3) Openness, 4) Autonomy of the Internet, and 5) Collaboration of Various Stakeholders
- With philosophy of promoting Cybersecurity Ecosystem, promote cybersecurity with following approaches: 1) Mission Assurance, 2) Risk Management, and 3) Participation, Coordination and Collaboration of all people.

Measures for Achieving Goals

Socio-Economic Vitality and Sustainable Development

1. Cybersecurity as Value Creation Enabler
2. Realizing Supply Chain Generating Value from Diverse Connection
3. Creation of Secured IoT Systems

Safe and Secure Society for the People

1. Proactive Cyber Defense and Efforts to Combat Cyber Crime
2. Critical Infrastructure Protection through PPP
3. Enhancing Security Measures on Nat'l Government
4. Cybersecurity at Academia and Research Institutes
5. CS for Tokyo 2020 envisioning "beyond 2020"
6. New Information Sharing & Collaboration Framework
7. Enhancing Readiness on Massive Cyberattack Crisis

Peace and Stability of Int'l Community and National Security

1. Commitment to Free, Fair and Secure Cyberspace
2. Strengthening Capabilities of Defense, Deterrence and Situational Awareness
3. International Cooperation and Collaboration

Crosscutting Measures

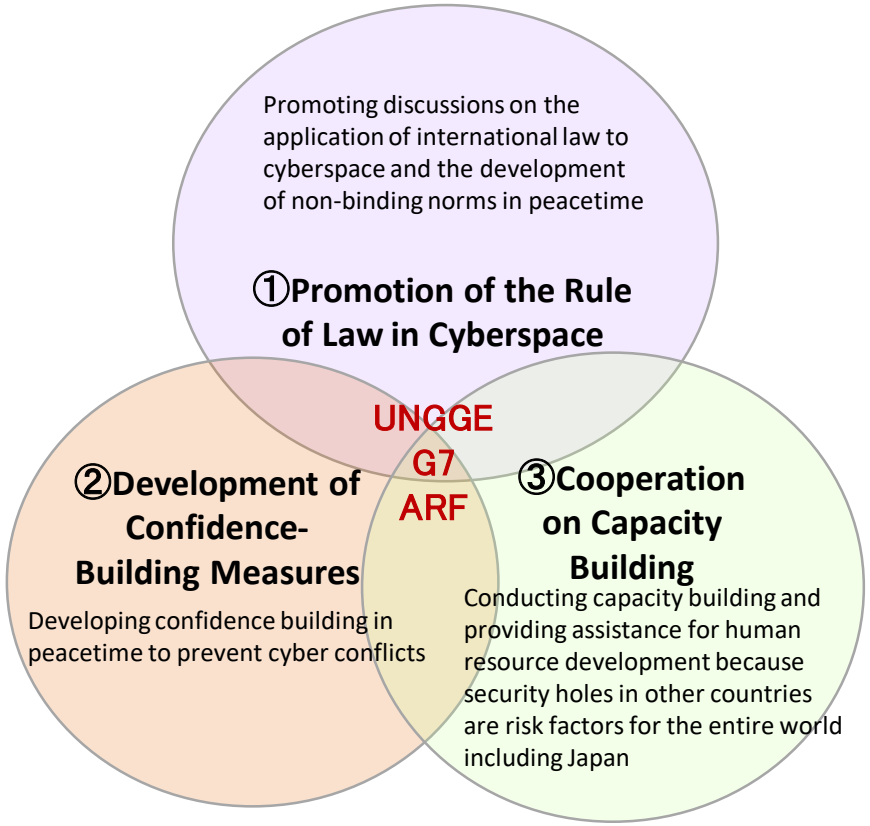
- Human Resource Development
- R&D Promotion
- Cyber Hygiene Full Participation of All Stakeholders

NISC, as the secretariat of the Cybersecurity Strategic Headquarters, plays a leading role, enhancing whole government approach, public private partnership.

Japan's Cyber Security Diplomacy – Three pillars

MOFA

➢ With the three pillars consisting of 1) promotion of the rule of law in cyberspace, 2) development of the confidence-building measures and 3) cooperation of capacity building, Japan aims to further contribute to the peace and stability of the Asia-Pacific region as well as the international community.



1 Partnerships and dialogues with other countries

(1) Japan has conducted bilateral dialogues on cyber with 11 countries (the US, Australia, the UK, France, Russia, India, ROK, Israel, Estonia and Ukraine).

(2) Japan also has had dialogues on cyber with the EU and ASEAN as well as within the Japan-China-ROK and Japan-US-ROK trilateral frameworks.

2 Major Global/Regional Frameworks

(1) United Nations Group of Governmental Experts (UNGGE): Governmental cyber experts from different countries discuss issues such as the rule of law and confidence-building in cyberspace within the framework of the UN. Since 2004, five sessions have been held.

(2) G7 (Summit Meeting and Foreign Ministers' Meeting): The G7 leaders decided to establish a new working group on cyber at Ise-Shima Summit 2016.

(3) G20: Cyber was one of the agendas and mentioned in the joint statement.

(4) ASEAN Regional Forum (ARF): The forum has held workshops on cyber and established a new Inter-sessional Meeting on Security of and in the Use of Information Communications Technologies(ARF-ISM on ICTs Security).

(5) Global Conference on Cyber Space (GCCS) (so called the London Process): Minister-level participants comprehensively discuss various issues on cyber.

*In addition, there are a number of track 1.5 dialogues and symposiums sponsored by the non-governmental sector.

NDPG and MTDP

防衛省・自衛隊 MINISTRY OF DEFENSE

On December 18th, 2018, the Government of Japan (GOJ) formulated the new National Defense Program Guidelines (NDPG) and the Medium Term Defense Program (MTDP).

◆ Position and significance

○ The National Defense Program Guidelines (NDPG) is formulated in line with National Security Strategy (NSS), which sets forth **Japan's basic defense policy, the function and roles Japan's defense capability, organizational objects for and the target level of specific organization of self-defense forces**, etc.

○ The Medium Term Defense Program (MTDP) is a defense program formulated for the five-year time frame based on the target level of defense capability set forth in the NDPG. The MTDP will build out a plan for maintaining and operating defense capability for each fiscal year through to FY 2023.

◆ Relationship between the NSS, NDPG, MTDP and Annual Budget

National Security Strategy (NSS)

Basic policy for national security, centered on foreign policy and defense policy (Approximately 10-year time frame)

↓ Formulate based on NSS

National Defense Program Guidelines (NDPG)

Sets forth the form and required level of defense capability (Approximately 10-year time frame)

↓ Accomplish the target level of defense capability

Medium Term Defense Program (MTDP)

Details the total cost (limit) over five years and inventorizes key capital equipment

↓ Budgeting and embodiment as projects

Annual Budget

By examining the environment, etc., budget the necessary cost for each fiscal year

NDPG's Objective

防衛省・自衛隊 MINISTRY OF DEFENSE

○ At present, security environment surrounding Japan is changing at extremely high speeds.

○ In strengthening its defense capability, Japan must squarely face the aforementioned realities of national security and ensure necessary and sufficient quality and quantity so as to build a truly effective defense capability that does not lie on a linear extension of the past.

○ In particular, it has become essential that Japan achieve superiority in new domains, which are space, cyberspace and electromagnetic spectrum; Japan needs to engage in a transformation at a pace that is fundamentally different from the past towards to build a new defense capability that combines strengths across all domains.

○ Japan's fulfillment of its responsibility as a sovereign nation is a foundation upon which to further enhance the ability of the Japan-U.S. Alliance, cornerstone of Japan's national security, to deter and counter threats, and to strategically promote security cooperation.

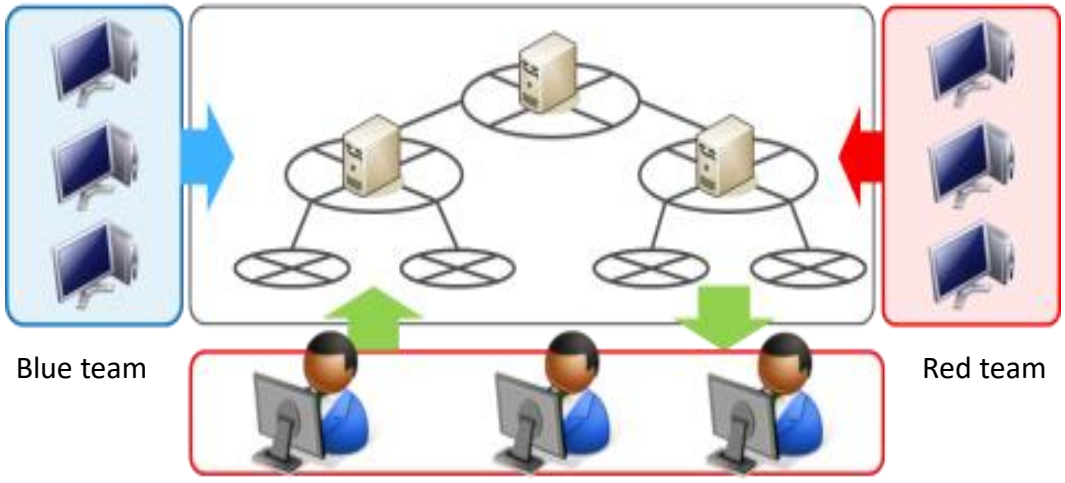
Capability to disrupt, during attack against Japan, opponent's use of cyberspace for the attack.

防衛省・自衛隊 MINISTRY OF DEFENSE

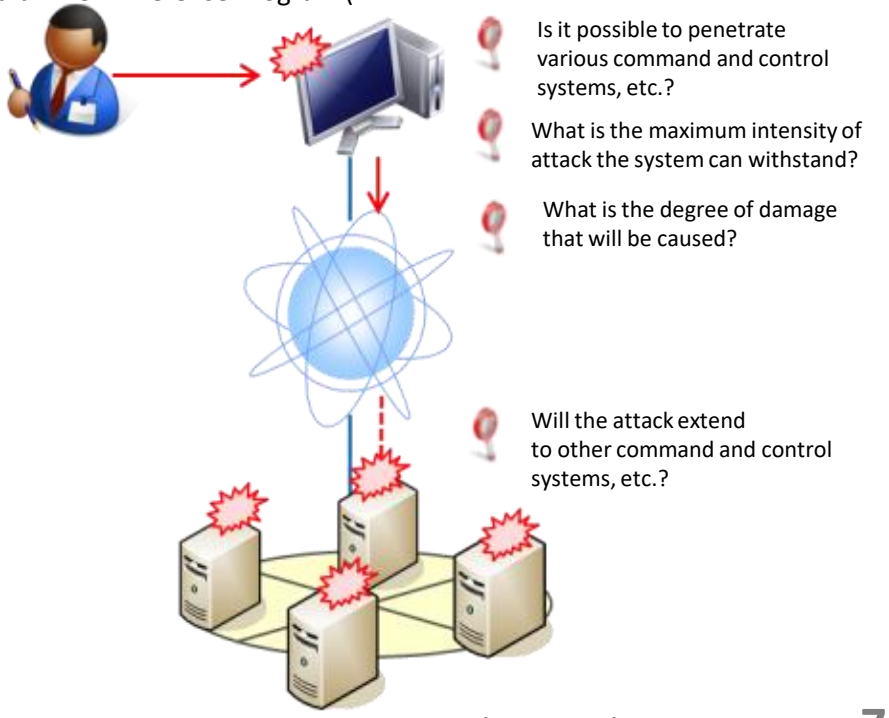
- On the assumption that MOD/SDF possibly needs to disrupt, during attack against Japan, opponent's use of cyberspace for the attack based on the previous Medium Term Defense Program* , MOD/SDF has enhanced investigation and analysis functions of malware, developed practical cyber exercise environment simulating SDF's command and control systems, and conducted vulnerability inspection of the SDF' command and control systems by using the same methods as actual attacks (penetration test) .
- Under the banner of the new National Defense Program Guidelines clearly stating the acquisition to capability to disrupt, during attack against Japan, opponent's use of cyberspace for the attack, MOD/SDF attempts to build such capability through a wide range of efforts.

*" Through its efforts to secure response capabilities in cyberspace where attackers have an overwhelming advantage, the SDF may consider the acquisition of capabilities to prevent them from using cyberspace." (Medium Term Defense Program (FY 2019 - FY 2023))

Simulation of command and control systems



Practical cyber exercise environment (concept)



Penetration test (concept)

National Defense Program Guidelines for FY2019 and beyond – Excerpt of Cyber Related Descriptions

防衛省・自衛隊 MINISTRY OF DEFENSE

Ⅲ. Japan's Basic Defense Policy

3. Strengthening security cooperation

(2) Responding to global issues

Regarding the use of cyber domain, Japan will enhance its partnership and cooperation with relevant countries through measures such as sharing views on threat awareness, exchanging views on response to cyber attacks, and participating in multilateral exercises.

Ⅳ. Priorities in Strengthening Defense Capability

2. Priorities in strengthening capabilities necessary for cross-domain operations

(1) Acquiring and strengthening capabilities in space, cyber and electromagnetic domains

In order to realize cross-domain operations, SDF will acquire and strengthen capabilities in new domains, which are space, cyberspace and electromagnetic spectrum by focusing resources and leveraging Japan's superb science and technology. In doing so, SDF will strengthen and protect command, control, communications and information capabilities that effectively connect capabilities in all domains including the new ones.

b. Capabilities in cyber domain

Information and communications networks that leverage cyberspace are a foundation for SDF's activities in various domains, and attack against them seriously disrupts organized activities of SDF. In order to prevent such attack, SDF will continue to strengthen capabilities for persistent monitoring of command and communications systems and networks as well as for damage limitation and recovery. In addition, SDF will fundamentally strengthen its cyber defense capability, including capability to disrupt, during attack against Japan, opponent's use of cyberspace for the attack.

In so doing, SDF will significantly expand its human resources with specialized expertise and skills, and take into consideration its contributions to whole-of-government efforts.

National Defense Program Guidelines for FY2019 and beyond – Excerpt of Cyber Related Descriptions

Ⅴ. Organization of Self-Defense Forces

1. Joint operation to realize cross-domain operations

(1) In order to further promote joint-ness of GSDF, MSDF and ASDF in all areas, SDF will strengthen the Joint Staff Office's posture designed for effective SDF operations and for new domains, thereby enabling swift exercise of SDF's capabilities. SDF will examine future framework for joint operation. SDF will also work to flexibly leverage personnel of each SDF service through such efforts as building posture for force protection and damage recovery with an eye on mutual cooperation among SDF services.

(3) SDF will maintain a cyberspace defense unit as an integrated unit in order to conduct persistent monitoring of SDF's information and communications networks as well as to fundamentally strengthen cyber defense capability, including capability to disrupt, during attack against Japan, opponent's use of cyberspace for the attack.

Medium Term Defense Program (FY2019 – FY2023) – Excerpt of Cyber Related Descriptions

II. Reorganization of the Major SDF Units

1. In order to build a structure that is capable of realizing cross-domain operations including new domains, which are space, cyberspace and electromagnetic spectrum, SDF will strengthen the Joint Staff's posture designed for effective SDF operations and for new domains, thereby enabling swift exercise of SDF's capabilities. For the future framework for joint operations, SDF will take necessary measures after considering how to conduct the operation of organizations in which the functions in the new domains are operated unitarily, and come to conclusions after considering how the integrated structure should be during steady-state to appropriately execute instructions from the Minister based on the posture of the strengthened Joint Staff. SDF will also work to flexibly leverage personnel of each SDF service through such efforts as building posture for force protection and damage recovery with an eye on mutual cooperation among SDF services.

   SDF will establish 1 squadron of cyber defense unit as joint unit in order to fundamentally strengthen cyber defense capabilities, including capability to disrupt, in the event of attack against Japan, opponent's use of cyberspace for the attack as well as to conduct persistent monitoring of SDF's information and communications networks.

Medium Term Defense Program (FY2019 – FY2023) – Excerpt of Cyber Related Descriptions

III. Major Programs regarding SDF's Capabilities

1. Priorities in Strengthening Capabilities Necessary for Cross-Domain Operations

(1) Acquiring and Strengthening Capabilities in Space, Cyber and Electromagnetic Domains

(B) Capabilities in Cyber Domain

SDF aims to persistently ensure sufficient security against cyber attack and acquire capability to disrupt, opponent's use of cyberspace in the event of attack against Japan. With consideration to enhancing joint functions and efficient resource allocations, SDF will establish the necessary environment by such measures as expanding the structure of cyber defense squadron and other units, enhancing the resiliency of the C4 systems of SDF, strengthening capabilities of information gathering, research and analysis, and developing a practical training environment that can test SDF's cyber defense capability. In addition, SDF will strive to keep abreast of the latest information including cyber-related risks, counter measures and technological trends, through cooperation with the private sector, and strategic talks, joint exercises and other opportunities with the ally and other parties.

As the methods of cyber attack are becoming increasingly sophisticated and complicated, securing personnel with expertise on a continuing basis is essential. SDF plans to develop personnel with strong cyber security expertise, through efforts such as improving the in-house curriculum for specialized education, increasing learning opportunities at institutions of higher education at home and abroad, and conducting personnel management that cultivates expertise. In addition, SDF will strengthen the cyber defense capability by utilizing superior outside expertise.

In order to enable a comprehensive response through a whole-of-government approach in cyber domain, MOD/SDF seeks to enhance close coordination with relevant ministries and agencies, etc. by providing knowledge and MOD/SDF personnel on a steady-state basis, and enhance training and exercises.

Establishment of the Cybersecurity Council

Second Amendment of the Basic Act on Cybersecurity was enacted on December 2018.

※ Effective on April 1,2019

Overview

- The Cybersecurity Council was established to enhance the discussion among relevant stakeholders in public and private sector to promote cybersecurity.
- The Act imposes **obligation** of **confidentiality** and **information sharing** on the members of the Cybersecurity Council.

The Cybersecurity Council

Council's Secretariat (NISC/Specialized Agencies)

Experts and other relevant entities

Strategic and prompt sharing and exchanging of cybersecurity-related information acquired from members

National Government Bodies	Local Governments	Critical Infrastructure Operators	Cyber Business Entities (Security and system solutions vendors, etc.)	Academia and Research Organizations
Implementation of measures	Implementation of measures	Implementation of measures	Implementation of measures	Implementation of measures

Promotion of Cybersecurity

Contribution to (1) socio-economic vitality and sustainable development, (2) people's safe and secure society, and (3) peace and stability of international community and national security

Cooperation ⇔ Relevant Foreign Parties(Public and Private)

Operational rules of the Cybersecurity Council

Back Ground	・Need to enhance information sharing in addition to removing barrier of information sharing through amendment of the act
Solution	・Establishing a Task Force (TF) composed of members who have ability and willingness for active information sharing
Merit to be a Task Force member	・Increasing accuracy of threat information through the cross-check and feedback among members ・Enabling TF members to obtain information shared only within the TF by ensuring give-and-take principle

- ✓ 1st category members (specialized agencies and security vendors) cross-check threat information
- ✓ 2nd category members give feedback to 1st category members
- ✓ Mitigation measures are provided to general members

Cybersecurity Policy for CIP (4th Edition) (April 2017, Revised July 2018)

Promoting CIP through public-private partnership

On the basis of the concept of mission assurance, in order to safely and continuously provide critical infrastructure services(CISs) and to avoid serious effects on the national life and socioeconomic activities from CISs outages resulting from cyber-attacks, natural disasters or other causes, all stakeholders should protect the critical infrastructures by reducing the occurrence of CISs outages as much as possible and by ensuring prompt recovery from outages.

Critical Infrastructures (14 sectors)

- Info. & comm.
- Finance
- Aviation
- Airport
- Railway
- Electric power supply
- Gas supply
- Gov. & admin. (incl. municipal government
- Medical
- Water
- Logistics
- Chemical industries
- Credit card
- Petroleum industries

【NISC】 coordination & cooperation

Responsible ministries for critical infrastructure (5 ministries)

- FSA [Financial]
- MIC [Info & comm, Admin]
- MHLW [Medical, Water]
- METI [Electric power supply, Gas, Chemical, Credit card, Petroleum]
- MLIT [Aviation, Airport, Railway, Logistics]

Organizations concerned

- Cybersecurity related ministries [MIC, METI, etc.]
- Crisis management ministries [NPA, MOD, etc.]
- Disaster prevention related ministries [CAO, ministries, etc.]
- Cybersecurity related agencies [NICT, IPA, JPCERT, etc.]
- Cyberspace-related operators [Various vendors, etc.]

This Cybersecurity Policy

Maintenance and promotion of the safety principles

Promoting continual improvement of the "guidelines" of measures that are most necessary from a cross-sectoral perspective, and the "safety principles" in each sector.

Enhancement of information sharing system

Enhancing the public-private and cross-sectoral information sharing system by diversifying the contact formation, defining the sharing of information, etc.

Enhancement of incident response capability

Enhancing the overall CISs outages response system by the implementation of exercises and collaboration between exercises and trainings, etc. performed under public-private partnership

Risk management and preparation of incident readiness

Promoting comprehensive management including preparation of incident readiness such as risk assessment, establishment of contingency plans by CI operators, etc.

Enhancement of the basis for CIP

Review of the protection scope, promoting the public relations activities and international cooperation, appeal to top management, promotion of developing human resources

Cybersecurity Policy for CIP (4th Edition)

(Adopted April 2018)
(Revised July 2018)

1. Points of Revision

◆ Mission Assurance: Promotion of actions to reduce risks of critical infrastructures' service outage caused by natural disasters, cyber-attacks, etc. and ensuring resilience in order to provide CI services safely and continuously, based on active and firm commitment of management executives.

◆ Envisioning Tokyo 2020: Essential services for organizing the Olympic and Paralympic games shall be secured.

2. Challenges

◆ CI operators are taking measures, but still have some challenges on Check & Action in PDCA cycle.
◆ Improve information sharing not only IT but also OT (Operational Technology) and promote incident readiness.
◆ Continue and improve provision of information to the nation through analysis and cooperation with various entities all over the world.

3. Policy Priorities

(1) Promotion of Leading Activities (Classification)

- Enhancing activities of leading sectors (such as electric power supply, information & communication services, and financial services), which other CI services highly depend on.
- Encouraging other CI operators to follow such leading activities for cybersecurity.

(2) Enhancement of Information Sharing Structure beyond the Olympic and Paralympic Games

- Introducing severity scale for CI service outages.
- Diversifying communication modality and channels (anonymization, sharing thru CEPTOAR* Secretariat and/or CIP supporting agencies) and breaking the barrier of information sharing; studying how to gather cross-sectoral information to the Cabinet Secretariat.
  *Capability for Engineering of Protection, Technical Operation, Analysis and Response
- Developing information sharing system for automated, labor-saving, swift and reliable operation (also envisioning to use it as hotline among stakeholders).
- Including OT, IoT, etc. in the scope of information sharing.
- Enhancing CIP by exercises and penetration tests.
- Expanding the protection scope as "cross-cutting sector-wide" including supply chain.

(3) Promotion of Incident Readiness Based on Risk Management

- Improving risk assessment in CI operators by providing NISC's "risk assessment guideline for mission assurance" and workshops.
- Promoting incident readiness of CI operators including BCP and contingency plan.
- Encouraging CI operators to conduct cybersecurity internal audit including monitoring and review, referring to NISC's risk assessment guideline.

4. Duration

◆ 4th Edition will cover by the end of the Olympic and Paralympic games, and will be revised even within the period if necessary.

Common Standards for Government Agencies

- **Common Standards Group for Information Security Measures for Government Agencies and Related Agencies** (hereinafter "the Common Standards") is a common framework to uniformly raise the level of information security for all governmental ministries, agencies and related agencies, as the "baseline" standard.
- **Government Agencies** should develop its own security policy on the basis of the Common Standards and implement it through their plan, taking duly into account their specificity.

Cybersecurity Strategic Headquarters

- Decides and revises the Common Standards
- Directs the implementation by the ministries and advises to improve

CISO Council

NISC

- Oversees objectively and uniformly the status of implementation
- Develops and revises the guidelines

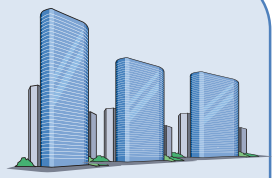
Common Standards

Lecture & Exercise

Status of implementation
Incident information

Management audit
Penetration test
Helps incident handling

Governments
IAAs
Special Corps.
(Designated only)



Plan
- Develops the security policy and the promotion plan

Do
- Training
- Technical measures
- Other measures

Check/Act
- Review/internal audit
- Improvement
- Evaluation/revise
- Re-allocation of resources

PDCA

Cybersecurity Operation

National Center of Incident Readiness and Strategy for Cybersecurity

Government Security Operation Coordination Team (GSOC)

Functions:
- Real-time government-wide monitoring (24/7)
- Warning & Advice: Enhancement of governmental response capabilities by accurate and prompt information sharing
- Malware analyses
  Information gathering on various risks

Monitoring

GSOC

Collaboration

CYber incident Mobile Assistance Team (CYMAT)

- CYMAT consists of staffs with advanced experiences and knowledge on information security, dispatched by governmental bodies.
- CYMAT deals with information security incidents that require government-wide responses in the event or potential risks of cyber attacks concerning information system failures of the entities assisted by CYMAT.
- Functions:
  - Situational awareness to get an accurate understanding of what is happening
  - Technical assistance and advice for damage control, recovery, and preventive measures
  - Activities in usual times to improve incident response capabilities (implementing workshops, training, etc.)

Assistance

Providing information on detected incidents & advices

Report on incidents

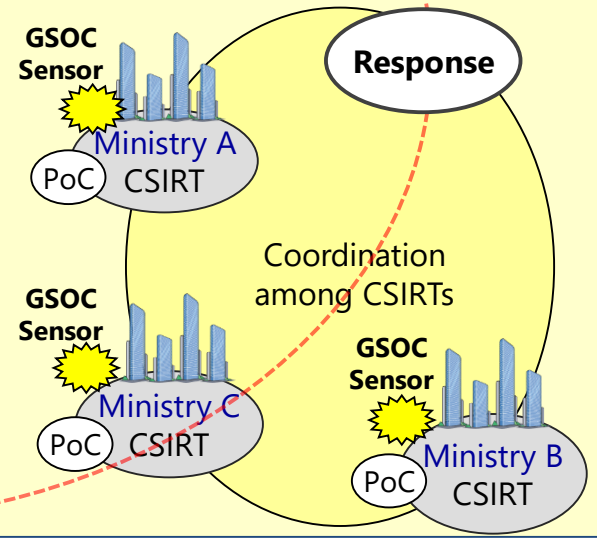
Request for emergency assistance

Technical assistance and advice

Collaboration, information sharing

CSIRTs of Ministries (Including IAAs and SC/Acs)

- System for smooth damage control and quick recovery in the case of information security failures or incidents at governmental bodies
- Functions:
  - Information gathering and analyses on incidents
  - Risk management for emergency response
  - Report/communications to Chief Officers, etc.
  - Staff education and training
  - Collaboration with relevant organs



Private CSIRTs, etc.

Overview of Interagency Agreement for Government Procurement of IT system, Equipment, and Services and Procurement Procedure

1. Scope

The IT system, equipment, and services judged to fall into following categories by each ministry through the consultation with NISC and National Strategy Office of IT

a. The system that deals with information regarding national security and public safety
b. The system treating confidential information or sensitive information, the breach of which causes social or economic loss
c. The system dealing with a large volume of personal information such as social security number
d. The foundation system such as LAN, the disruption of which causes serious effect on the ministry's operation
e. The system with high running cost

2. Effectuation

From April 1st 2019

3. Procurement Process

Above systems will be procured through the comprehensive scoring auction which takes various factors into consideration as well as price. Each ministry can obtain necessary information by issuing RFI (Request for Information) or RFP (Request for Proposal).

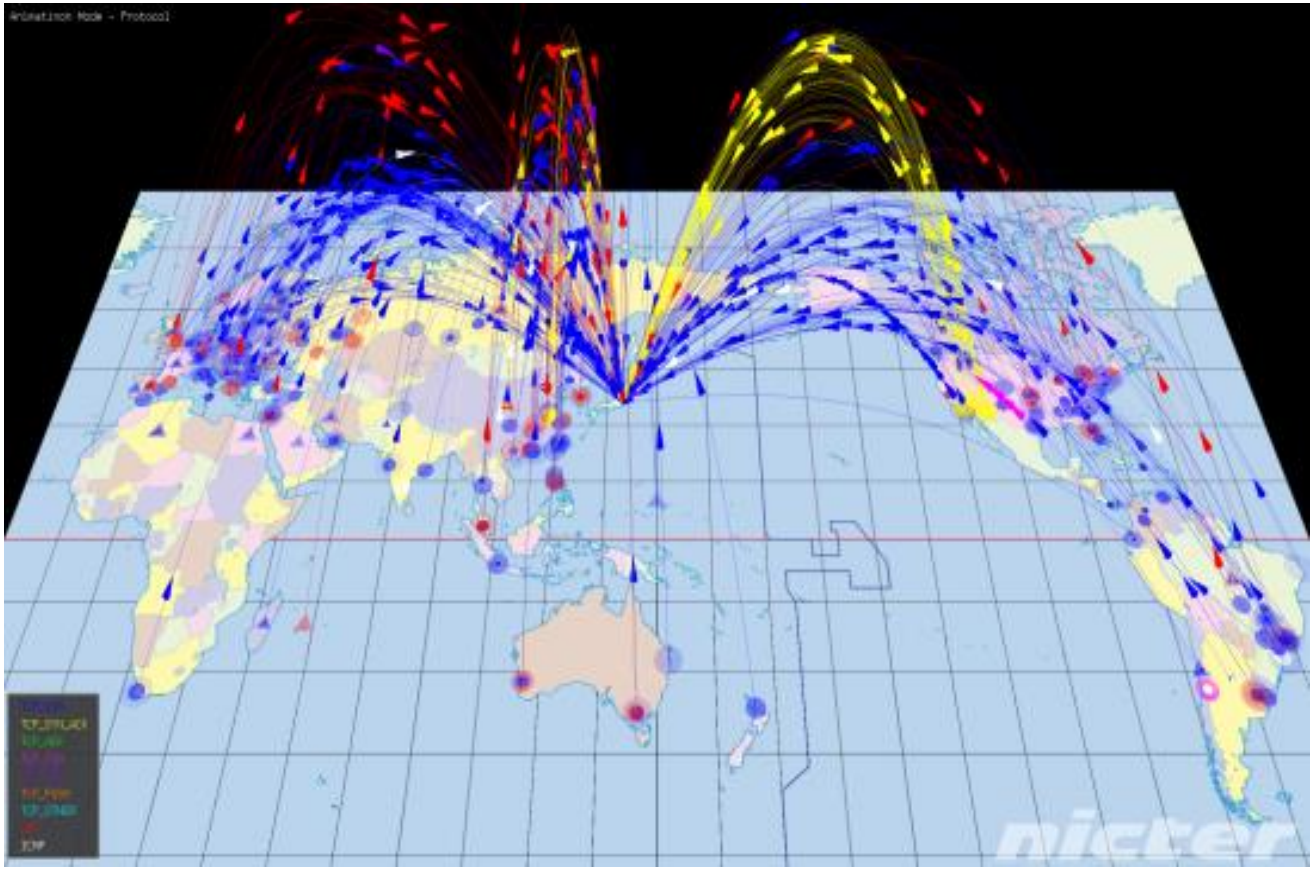
4. Advice by NISC and National Strategy Office of IT

When necessary, each ministry should consult with NISC and National Strategy Office of IT about appropriate measures to ensure cybersecurity of its system through the procurement process.

Cyber Attacks Observed by NICTER

MIC

National Institute of Information and Communications Technology (NICT) is observing cyber attacks globally by monitoring 300,000+ unused IP addresses (darknet).

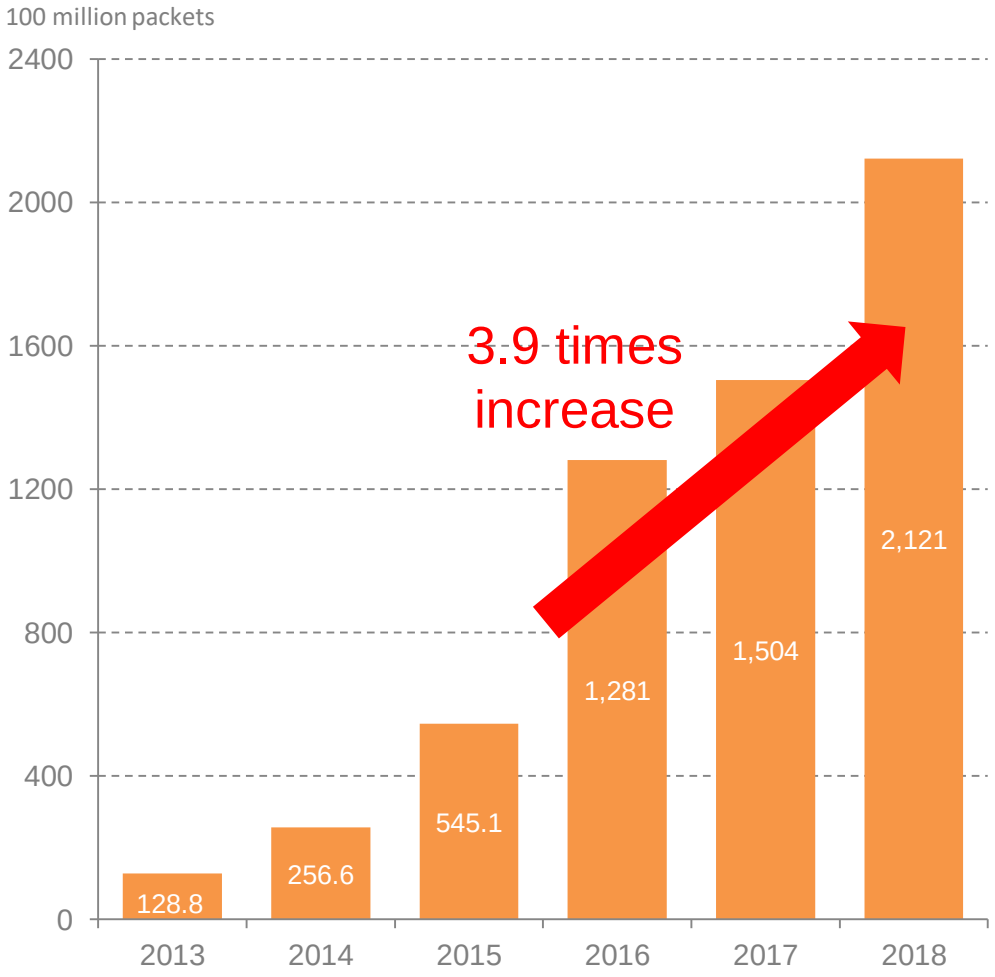


TCP SYN TCP SYN/ACK TCP ACK TCP FIN
TCP RESET TCP PUSH TCP Other UDP ICMP

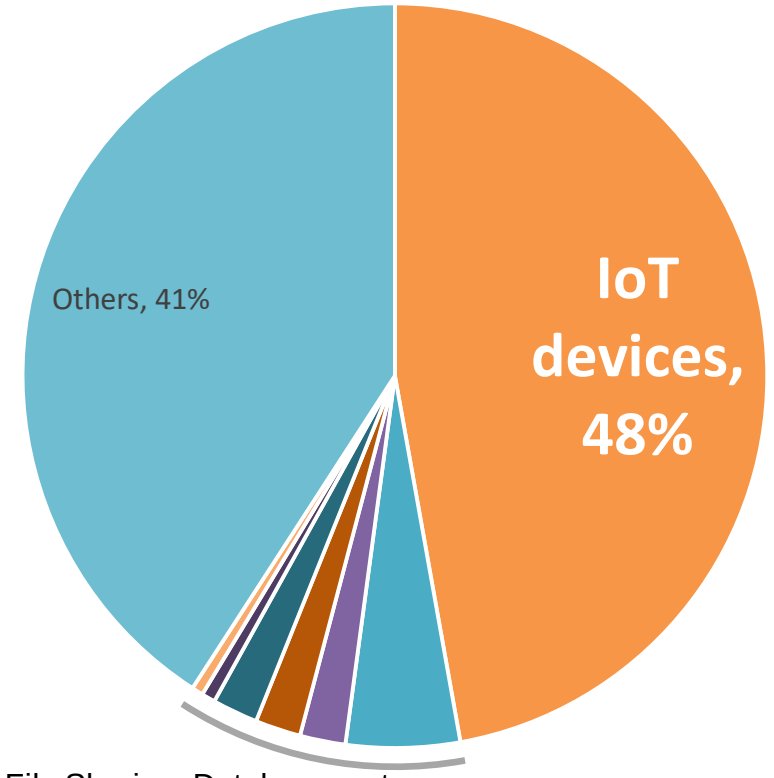
Attacks on IoT Devices (Observed by NICTER)

IoT Devices: Router, Web Camera, Sensor, etc.

MIC



Number of cyberattacks observed by NICTER in one year



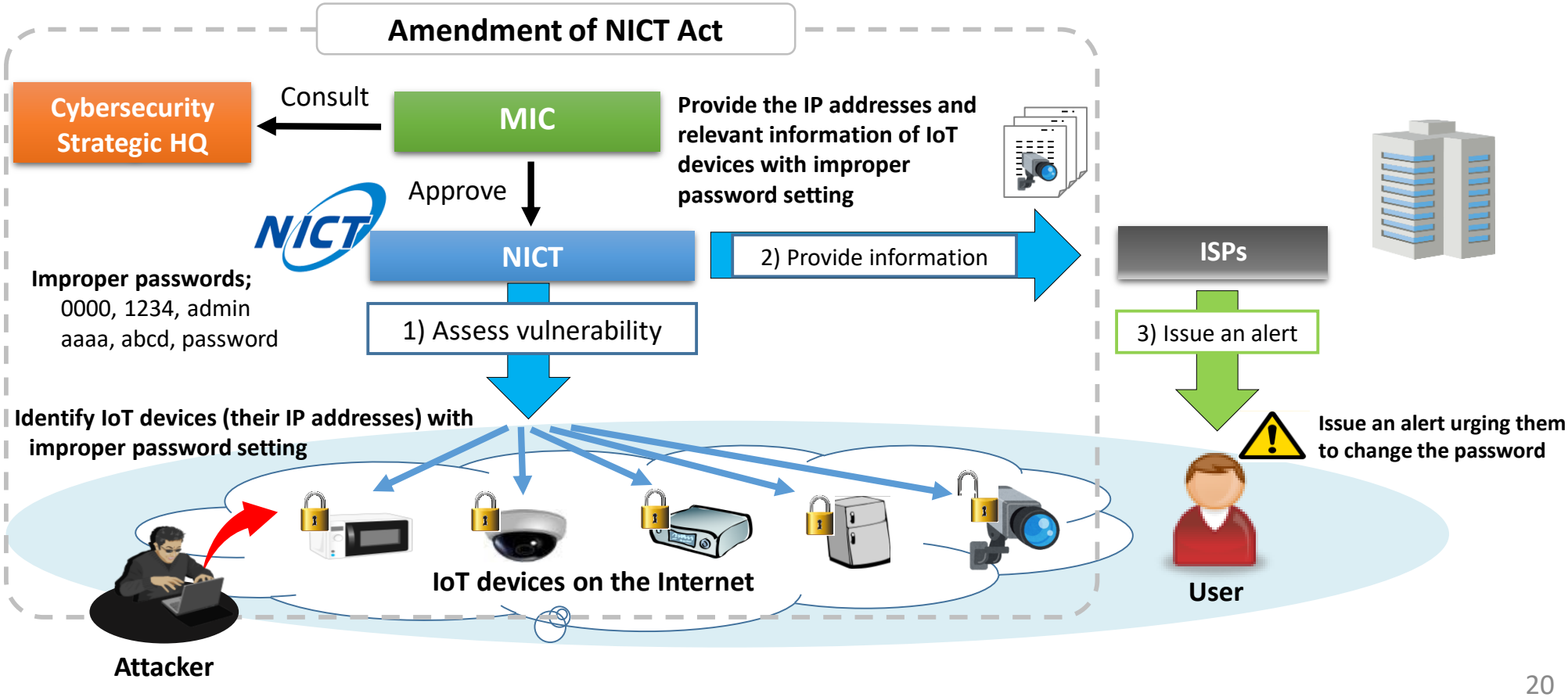
Targets of cyber attacks observed by NICTER

About half of attacks targeted at IoT devices!

Identify IoT Devices with Improper Password Settings

MIC

Due to the sophistication of cyber attacks using IoT devices, the amendment of the NICT Act was passed the diet in May 2018. The act enables NICT to scan IoT devices on the Internet and identify IoT devices with improper password setting.



Project to Alert Users of IoT Devices Infected with Malware

Along with NOTICE, MIC and the NICT, in cooperation with ISPs, conduct the project to identify devices infected with malware by using NICTER system and notify the ISPs so that they can alert users of the infected devices from mid June 2019.

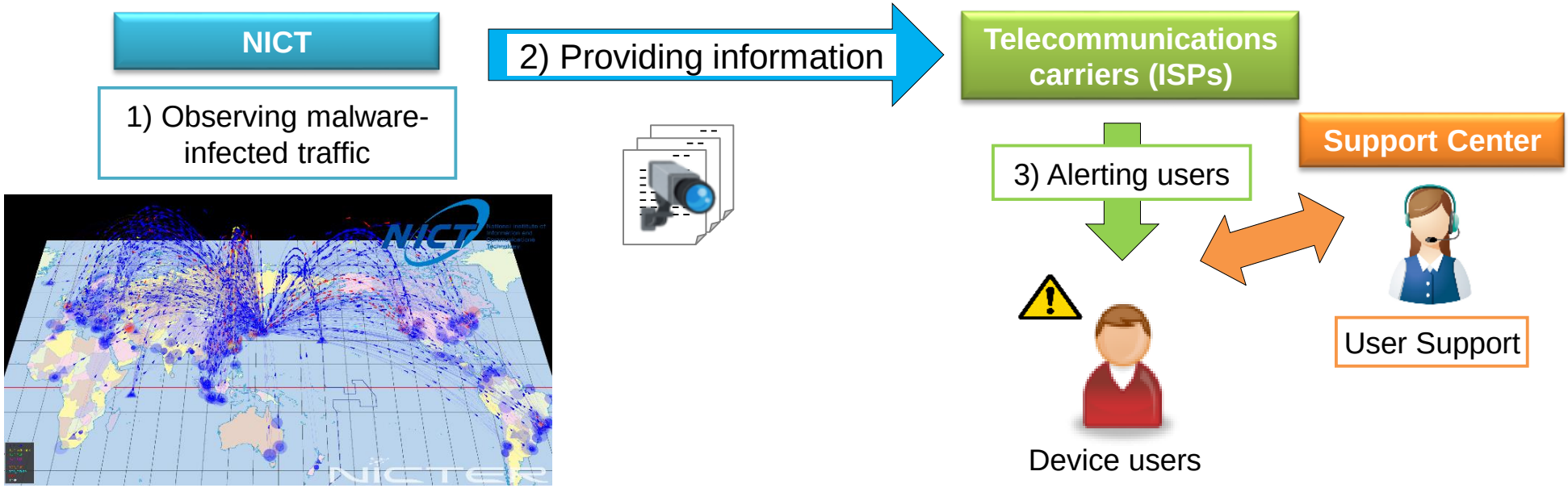
MIC

<Overview of the project>

(1) NICT identifies the devices generating the malware-infected traffic by using NICTER system.

(2) NICT provides the information of the malware infected devices **to ISPs**.

(3) The ISPs identify the users of the devices **and alert users**.



Progress on the Projects

MIC

Among 200 million IP addresses in Japan, approximately 90 million IP addresses managed by 33 ISPs that are participating in the projects have been investigated.

(1) Results of NOTICE

Number of IP addresses in which **ID and password could be entered** → Approx. 31,000-42,000

In the above, the number of those which were **successfully logged-in** to with **weak password settings** and were **subject to user alert** → Total 147

(2) Results of the project to alert users of malware-infected IoT devices

Number of IP addresses which seem to be **infected with malware** and were **subject to user alert** → 112-155 per day

The number of Internet Service Providers participating in the project is 33.
In addition to these measures, a proactive measure is required.

(⇒next page)

Proactive measure for IoT security

MIC

Amendment of the Technical Condition of Terminal Equipment for IoT Security

- **Terminal equipment** that is directly connected to telecommunication network through internet protocol **is required to have**:
  1) access control on the remote control function,
  2) feature to **encourage its user to change the default IDs/passwords**
  3) firmware update feature for the future security fixes,
  or any equivalent/better security measures to/than above.
- The requirement does not apply to personal computers or smartphones that are generally protected by other security measures such as anti-virus software.
- MIC published the guideline for the security requirements of the Technical Condition, which describes the scope of device types, details of the requirements, etc.

Schedule

- The amended Technical Condition will be enforced on April 1, 2020.
  After this, the type approval will be given to only the terminal equipment that conform to the Technical Condition.

Cybersecurity Month Campaign (Feb. 1 - March 18, 2018 & 2019)

Cybersecurity Month 2018 focused “Analogue Hacking (social engineering),” which enables spear-phishing attacks penetrating people’s mind.

Kickoff Summit

The symposium commenced this year’s campaign inviting cybersecurity missionaries around the country on-site and via video-connection. The summit was lively casted on the net.

Collaboration with Pop-culture

(Updated 2019 version) Popular characters in an animation drama “Promised Neverland” are featured to raise awareness of cybersecurity.

Message from the Top

Chief Cabinet Secretary, the Chair of the Cybersecurity Headquarters, released a video message inviting people to consider cybersecurity.

NISC Caution and Alert Information

NISC posts cybersecurity information through SNSs targeting various generations.

Information Security Handbook

Easy-to-understand booklet with some Manga illustration to advocate risk and threats in the cyberspace.

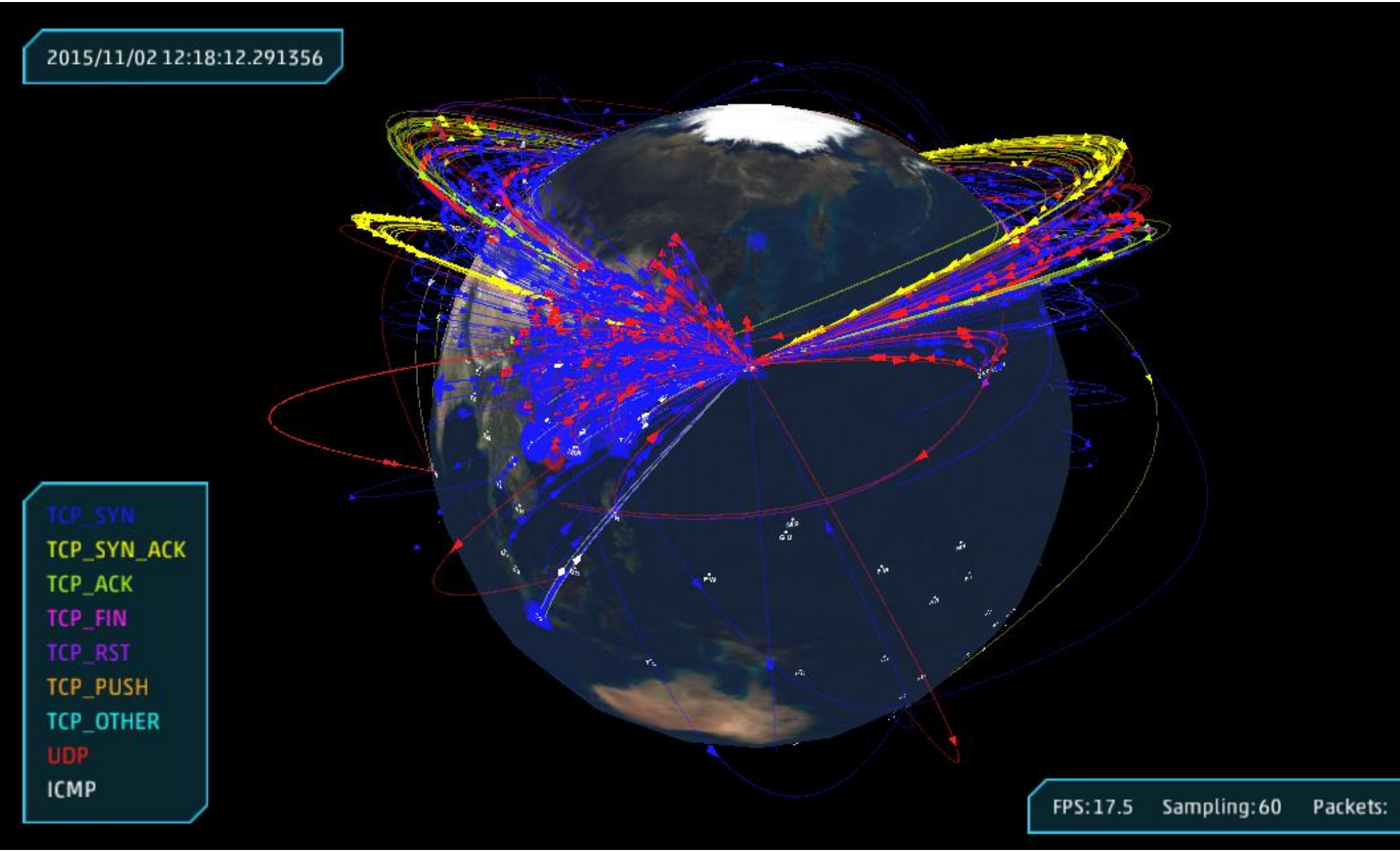
Columns by Cybersecurity Leaders

“Witness Analog Hacking! Akihabara 2018” Event

Cyber-attack demonstration, symposium talking about near-future world after cyber singularity takes place, etc. was featured for public awareness of cybersecurity.

NATIONAL 318 (CYBER) EKIDEN

Information Security Incident Handling Competition for Ministries.


2015/11/02 12:18:12.291356
TCP_SYN
TCP_SYN_ACK
TCP_ACK
TCP_FIN
TCP_RST
TCP_PUSH
TCP_OTHER
UDP
ICMP
FPS:17.5
Sampling:60
Packets:

Thank you