

REPORT OF THE SURVEY ON AWARENESS RAISING ACTIVITIES FOR CYBERSECURITY IN JAPAN

FEBRUARY 2022

JAPAN INTERNATIONAL COOPERATION AGENCY (JICA)

JAPAN DEVELOPMENT SERVICE CO., LTD. (JDS)

GP
JR
22-017

CONTENTS

1.	Executive Summary	1
2.	Policies and Related Organizations in Japan on Awareness Raising Activities of Cybersecurity..	1
2.1	Policies and Guidelines in Japan on Awareness Raising Activities of Cybersecurity.....	1
2.2	Organizations and Bodies related to Cybersecurity in Japan.....	4
2.3	National Budget on Cybersecurity in Japan.....	11
3.	Policy, Guideline and Practice regarding Cybersecurity Education in Japan	12
3.1	Cybersecurity Human Resource Development Program.....	12
3.2	A Guide to the Informatization of Education.....	12
3.3	Information Moral Education at Schools	13
3.4	Educational Materials for Schools in Japan	13
4.	Human Resources for Awareness Raising in Japan	13
4.1	Professional Certification in Japan	13
4.2	Non-certification-based Human Resource Development in Japan for Awareness Raising	16
5.	Overview of awareness raising activities in Japan.....	20
5.1	Public Seminars on Cybersecurity Awareness Raising	21
5.2	Private Seminars on Cybersecurity Awareness Raising.....	22
5.3	Tools and Contents on Cybersecurity Awareness Raising.....	23
5.4	Information Dissemination/Consultation Service.....	24
6.	Materials for Cybersecurity Awareness Raising in Japan.....	25
6.1	Web Portals/Information sites/Web Services.....	25
6.2	Textbooks/Materials	28
6.3	Manga/Cartoons.....	32
6.4	Videos/Animations	34
6.5	Game/E-learning/Simulation	40
7.	Experiences, Knowledge, and Issues related to Awareness Raising Activities in Japan	42
7.1	Awareness Survey on Ethics and Threats of Information Security Report.....	42
7.2	Survey Report on Security Trends in Corporate Organizations	43
7.3	Whitepaper on Crime (Ministry of Justice).....	44
8.	Characteristics of Awareness Raising Activities for each Target Audience in Japan.....	45
8.1	Overall Characteristics of Awareness Raising Materials in Japan	45
8.2	Issues on Child Protection in Japan.....	45
8.3	Cybersecurity of elderly people in Japan	46
9.	Strategies and Theories for Awareness Raising Activities in Japan	46
10.	Marketing Methods and Theories for Awareness Raising Activities.....	49
10.1	Why Marketing?	49
10.2	What is Marketing?.....	50
10.3	Overview of Marketing Process	52

10.4	Digital Marketing.....	66
11.	How to Measure the Effectiveness of Awareness Raising Activities	74
12.	Recommendations for Awareness Raising Activities in Vietnam	74
12.1	Learn from experiences in Japan.....	75
12.2	Setting the target segment in a time frame, but eventually carrying it out to the level where the entire nation is aware of it.....	75
12.3	Planning content that can involve earned media (third parties).....	75
12.4	Inducing synergy effects in awareness raising activities by bundling cybersecurity initiatives with other IT-related initiatives.....	75
12.5	Setting indicators that can be monitored at fixed points.....	75
12.6	Improving the cybersecurity literacy of government officials (including those in local governments)	76
Appendix 1: Worksheets for STP Analysis.....		77

LIST OF FIGURES AND TABLES

(Figures)

Figure-1	Structure of NISC Annual Report on Cybersecurity 2021	4
Figure-2	The Relationship of CSH, NISC, and IPA	5
Figure-3	Implementation Framework of NISC	7
Figure-4	The Scope of IPA Activities	8
Figure-5	GSOC System Overview	10
Figure-6	National Budget on Cybersecurity in Japan	11
Figure-7	Professional Certifications in Japan related to Cybersecurity	14
Figure-8	Overall Picture of Cybersecurity Helpers Project.....	17
Figure-9	Target Area and the Concept of Cybersecurity Helpers PoC in 2019	17
Figure-10	SMEs Participation by industry for Cybersecurity Helpers PoC (2019)	18
Figure-11	Target Areas of Cybersecurity Helpers PoC in 2020	18
Figure-12	Logo of the Cybersecurity Helpers.....	19
Figure-13	Card Design in the Game for Learning Suspicious Things on the Internet	40
Figure-14	Security Education and Awareness on Phishing Scams by Age Group in Japan	43
Figure-15	Damage Amount of Security Incidents in Japan	44
Figure-16	Increasing cybercrime cases in Japan (Whitepaper on crime).....	44
Figure-17	Manga Comedy to Promote Strong Password by IPA.....	45
Figure-18	Example of Smartphone Designed for Elderly People	46
Figure-19	Logo for Cybersecurity Awareness Raising (Know - Protect - Continue)	47
Figure-20	Overview of the Cybersecurity Awareness Raising Program	49
Figure-21	Examples of Marketing Approaches	50
Figure-22	Objective of Market Research for Business	53
Figure-23	Examples of Market Research Framework.....	54
Figure-24	Overview of STP Analysis	55
Figure-25	Example of Conventional Cases for Product/Service Positioning (PC Eyeglass).....	58
Figure-26	Example of Positioning Map for Cybersecurity Awareness Raising Activity	59
Figure-27	Standard Framework of Marketing Mix	60
Figure-28	Promotional Mix.....	63
Figure-29	Relation of KGI and KPI	65
Figure-30	Maturity Stage of Cybersecurity defined by JCIC.....	65
Figure-31	Example KGI/KPI for Awareness Raising activity in Vietnam	66
Figure-32	SMART Framework for Effective KGI/KPI Setting.....	66
Figure-33	Definition of Digital Marketing by Dentsu	67
Figure-34	Overview of Digital Marketing	67
Figure-35	The Three Changes due to Digitalization	67
Figure-36	Example of a Persona	69
Figure-37	Example of Customer Journey map.....	70

(Tables)

Table-1 Main Members of the “Kan-min Board” 9

Table-2 Example of Projects related to Awareness Raising 11

Table-3 10 Major Security Threats of 2021 29

Table-4 Short Animation Series “Cybersecurity Helpers Service” by IPA (2021) 34

Table-5 Short Animation Series “Let’s learn cybersecurity basics with piglet”
by IPA (2020) 34

Table-6 Short Video Series “Fraud Technique Verification” by IPA (2021) 35

Table-7 Short Video Series “Targeted Cyberattack” by IPA (2012~2016) 35

Table-8 Short Video Series “Skits - Learn before suffering from security incidents”
by IPA (2019) 36

Table-9 Other videos and animations for awareness raising by IPA 36

Table-10 Short Animation Series for Cybercrime Prevention by NPA (2019~) 37

Table-11 Short Video Series Aimed at Senior Citizens for Cybercrime Prevention
by NPA (2019~) 38

Table-12 Short Video Series “Threats in cyberspace – Now your company is targeted –”
(2016) 38

Table-13 Short Video Series Aimed at kids to Learn Risks on the Internet by NPA (2021)..... 38

Table-14 Short Animation Series “Smartphone/mobile phone case file” by KDDI 39

Table-15 Types of Data for Market Research 54

Table-16 Example of JCIC’s KPI for Cybersecurity Readiness 65

Table-17 Methods for Collecting Raw Data for Evaluation of Awareness Raising Activities.. 74

TABLE OF ABBREVIATED WORDS

Abbreviation	Definition	Japanese
CSIRT	Computer Security Incident Response Team	シーサート
CSH	Cybersecurity Strategy Headquarters	サーバーセキュリティ戦略本部
GSOC	Government Security Operation Coordination team	政府関係機関情報セキュリティ横断監視・即応調整チーム
IPA	Information-technology Promotion Agency, Japan	情報処理推進機構
JFY	Japanese Fiscal Year	年度
JASA	Japan Information Security Audit Association	日本セキュリティ監査協会.
JCIC	Japan Cybersecurity Innovation Committee	日本サイバーセキュリティ・イノベーション委員会
JNSA	Japan Network Security Association	日本ネットワークセキュリティ協会
KGI	Key Goal Indicator	重要目標達成指標
KPI	Key Performance Indicator	重要業績評価指標
METI	Ministry of Economy, Trade and Industry	経済産業省
MEXT	Ministry of Education, Culture, Sports, Science and Technology	文部科学省
MOJ	Ministry of Justice	法務省
NISC	National Center of Incident Readiness and Strategy for Cybersecurity	内閣サイバーセキュリティセンター
NPA	National Police Agency	警察庁
PTA	Parent-Teacher Association	PTA
Public-Private Board	Public-private joint committee for opinion aggregation on unauthorized access prevention measures	不正アクセス防止対策に関する官民意見集約委員会 (官民ボード)
SME	Small to Medium sized Enterprises	中小企業
STP	Segmentation, Targeting, Positioning	

1. Executive Summary

This report contains the result of survey on cybersecurity awareness raising activities as well as their materials and related policies/guidelines in Japan from Chapter 1 to Chapter 8. The report also presents marketing methods and theories for awareness raising activities (Chapter 9), how to measure the effectiveness of awareness raising activities (Chapter 10). Based on these contents, several recommendations for awareness raising activities in Vietnam are proposed in Chapter 11.

As for the cases in Japan, under the Basic Act on Cybersecurity (2.1.1), Cybersecurity Strategy Headquarters (2.2.1) prepares national strategies for cybersecurity, and delegates implementation of selected tasks to Information-technology Promotion Agency (2.2.3) under supervision of National Center of Incident Readiness and Strategy for Cybersecurity (2.2.2). A wide range of cybersecurity awareness activities including promotional events, seminars, trainings, etc. are conducted both in public sectors and private sectors, often with collaborations between them (Chapter 5). Materials used for these activities in Japan include websites, textbooks, cartoons, videos/animations, games/simulations, and e-learning materials (Chapter 6).

The notable characteristics of awareness raising activities in Japan are frequent use of visual information including manga (cartoon) and animation (8.1). There is also a growing concerns of child online protection in Japan (8.2) and protection of elderly people from online scam (8.3).

Marketing methods and theories for awareness raising activities should begin with traditional marketing processes (10.3) such as market research and STP analysis, all the way to KGI/KPI setting which is the most important part for measuring the effectiveness of activities (Chapter 11). But digital marketing (10.4) is also indispensable for cybersecurity awareness raising in the digital era.

In conclusion, there are six recommendations for awareness raising activities in Vietnam based on the survey result (Chapter 12) including the selective learning of experiences in Japan and synergy effects in awareness raising activities by bundling cybersecurity initiatives with other IT-related initiatives.

2. Policies and Related Organizations in Japan on Awareness Raising Activities of Cybersecurity

2.1 Policies and Guidelines in Japan on Awareness Raising Activities of Cybersecurity

2.1.1 The Basic Act on Cybersecurity¹

Source: Government **Year:** 2014

This is the basis of all policies regarding cybersecurity awareness raising in Japan. The purpose of the Act is to promote the cybersecurity policy comprehensively and effectively by:

- Stipulating basic principles of national cybersecurity policy

¹ <http://www.japaneselawtranslation.go.jp/law/detail/?vm=04&re=01&id=2760>

- Clarifying the responsibilities of the national government, local governments, and other concerned public parties
- Stipulating essential matters for cybersecurity-related policies such as formulation of the cybersecurity strategy
- Establishing the Cybersecurity Strategic Headquarters (later became NISC)
- Promotion of Education and Learning, Public Awareness Raising: Article 22
- For the purpose of extensive public awareness raising and understanding about cybersecurity among people, the national government is to provide necessary measures including the promotion of education and learning, public awareness activities, and the dissemination of knowledge in the field of cybersecurity.
- In order to promote it, the national government is to provide necessary measures, including the implementation of events for public awareness and the dissemination of information on cybersecurity and the designation of a specific, focused campaign period to effectively promote cybersecurity activities

2.1.2 Cybersecurity Strategy²

Source: Cabinet decision / NISC **Target Year:** JFY 2021-2024

This is the national strategy for cybersecurity in Japan that is updated and renewed every three years by NISC (→2.2.2). The latest version covering JFY 2021-2024 was issued on September 28th, 2021. The strategy summarizes the goals and implementation policies of measures for the next three years on the cybersecurity-related policies of each ministry and agency. The policy approaches consist of the following four pillars:

- Enabling socio-economic vitality and sustainable development (Advancing DX with Cybersecurity)
- Realizing a digital society where people can live with a sense of safety and security
- Contributing to the peace and stability of the international community and Japan's national security
- Cross-cutting approaches to cybersecurity

In the area of awareness raising promotion, full participation of industry, academia, government, and the private sector is particularly emphasized since the government alone has limitations.

² <https://www.nisc.go.jp/eng/pdf/cs-senryaku2021-en.pdf>

2.1.3 International Strategy on Cybersecurity Cooperation (J-initiative for Cybersecurity)³

Source: NISC **Year:** 2013

This strategy covers the promotion of capacity building and awareness raising activities including trainings targeted at government and corporate cybersecurity managers and CSIRTs. There are three projects mentioned in this strategy as examples of international cooperation as follows.

- CSSC (Control System Security Center)⁴

Established in 2013 by a technology research association of infrastructure manufacturers and other companies, this center has security verification facilities for industrial control systems (such as small-scale mock plants to simulate electric power system, gas system, building automation, automaker, sewage treatment, smart community and chemical process automation) in response to increasing demand to secure the safety of information and communication technology systems controlling infrastructure. Members of the association conduct activities such as development of technology to enhance security of control systems, and capacity building for control system security personnel. CSSC plans to accept visits from stakeholders abroad, to provide training courses, and to organize international conferences.

- PRACTICE (Proactive Response Against Cyber-attacks Through International Collaborative Exchange)⁵

This project has been implemented since FY 2011 by internationally building a network to gather information related to cyberattacks and malware, etc. The project utilizes international conferences (bilateral and multilateral) and call upon organizations (internet service providers, universities, etc.) of various countries to collaborate in sharing information such as cyberattack monitoring data and analysis results and in conducting research and development.

- TSUBAME (International Network Traffic Monitoring Project)⁶

TSUBAME is a project for packet traffic monitoring system to observe suspicious scanning activities in the Asia Pacific and other regions. It aims to promote collaboration among mainly CSIRTs with a national responsibility in the Asia Pacific and other regions by using the common platform and enhance capability of global threat analyses by incorporating 3D visualization features to the common platform.

³ https://www.nisc.go.jp/eng/pdf/InternationalStrategyonCybersecurityCooperation_e.pdf

⁴ <http://www.css-center.or.jp/en/index.html>

⁵ https://www.soumu.go.jp/main_content/000544714.pdf

⁶ <https://www.apcert.org/about/structure/tsubame-wg/index.html>

2.1.4 Common guidelines for government agencies

Source: NISC / Cybersecurity Strategy Headquarters

Year: 2018

There are following common guidelines on cybersecurity measures for government agencies.

- Common Model of Information Security Measures for Government Agencies and Related Agencies⁷
- Common Standards for Information Security Measures for Government Agencies and Related Agencies⁸
- Guidance on Operations of Information Security Measures of Government Agencies and Related Agencies⁹
- Guidelines for developing countermeasure standards for government agencies¹⁰

2.1.5 Cybersecurity 2021 (NISC Annual Report)

NISC has issued the annual report on cybersecurity of Japan since 2010. The latest is 2021 issue (report of 2020 and plan for 2021)¹¹. This report consist of the sections shown in the figure below.

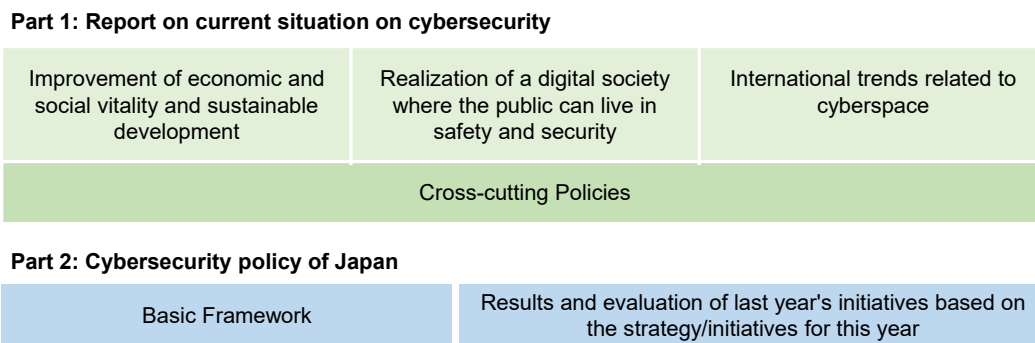


Figure-1 Structure of NISC Annual Report on Cybersecurity 2021

2.2 Organizations and Bodies related to Cybersecurity in Japan

2.2.1 Cybersecurity Strategy Headquarters¹²

The Cybersecurity Strategy Headquarters (CSH) was established in 2015 pursuant to the Basic Act of Cybersecurity (→ 2.1.1). Article 24 of the Act reads “For the purpose of effectively and comprehensively promoting Cybersecurity policies, the Cybersecurity Strategy Headquarters are to be established under the Cabinet”. Article 25 defines the functions of the Headquarters as follows.

- (i) Preparing the Cybersecurity Strategy and promoting its implementation.

⁷ <https://www.nisc.go.jp/eng/pdf/kihan30-en.pdf>

⁸ <https://www.nisc.go.jp/eng/pdf/kijyun30-en.pdf>

⁹ <https://www.nisc.go.jp/active/general/pdf/guide30.pdf>

¹⁰ <https://www.nisc.go.jp/eng/pdf/shishin30-en.pdf>

¹¹ <https://www.nisc.go.jp/active/kihon/pdf/cs2021.pdf>

¹² https://japan.kantei.go.jp/97_abe/actions/201502/10article4.html

- (ii) Establishing the standards of Cybersecurity measures for national administrative organs and Incorporated Administrative Agencies, and promoting implementation of the evaluation (including audit) of measures based on the standards and other measures taken pursuant to the standards.
- (iii) Evaluating countermeasures against critical cybersecurity-related incidents involving national administrative organs (including fact-finding activities to determine the cause or causes of incidents).
- (iv) Beyond the functions listed in the preceding three items, with respect to major cybersecurity policies: engaging in research and deliberation on program proposals; establishing cross-governmental plans, budget plans and guidelines of relevant administrative organs, the basic principles of program implementation as well as promoting the implementation of policy evaluation and other relevant policies; and carrying out overall coordination.

Under this Headquarters, two implementing organizations are established: NISC and IPA as shown in the figure below.

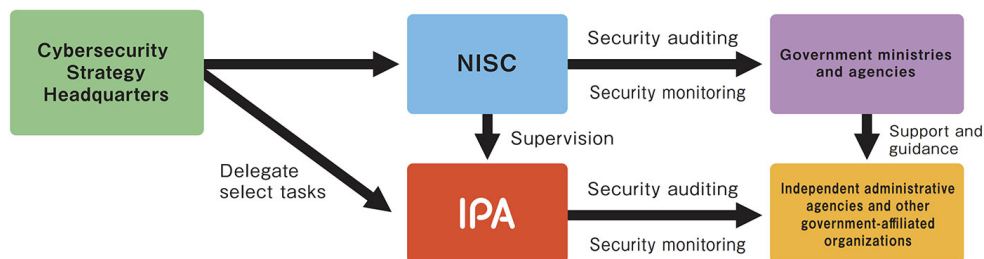


Figure-2 The Relationship of CSH, NISC, and IPA¹³

2.2.2 NISC (National Center of Incident Readiness and Strategy for Cybersecurity)¹⁴

NISC, which was established in 2015, was formerly called “National Information Security Center” since 2005 under the same abbreviation “NISC”, as a secretariat of the Cybersecurity Strategy Headquarters, working together with the public and private sectors on a variety of activities to create a “free, fair and secure cyberspace”. NISC plays the leading role as a focal point in coordinating intra-government collaboration and promoting partnerships between industry, academia, and public and private sectors.

NISC coordinates cybersecurity policy by formulating:

- 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.

¹³ <https://www.ipa.go.jp/files/000058630.pdf>

¹⁴ <https://www.nisc.go.jp/eng/index.html>

NISC assumes the role of a governmental CERT, and NISC and JPCERT/CC, as CERT covering private entities, work together as a national CERT.

NISC consists of the following seven groups. The main activities are as follows.

- **Strategy and Policy Planning Group**
Formulation of medium-to-long term plan on cybersecurity policy, and conducting research and analysis of cybersecurity technology trends, etc.
- **International Strategy Group**
Promotion of international cooperation on cybersecurity policy.
- **Planning and Security Audit for Government Entities Group**
Formulation and operation of unified standards for promoting information security measures of government agencies which is a basis of audit.
- **Integration and Coordination of Cybersecurity Information Group**
Collection of the latest information on cyberattacks and operation of the Government Security Operation Coordination team (GSOC).
- **Critical Infrastructure Protection Group**
Creation of public-private partnership in cybersecurity measures based on the Cybersecurity Policy for Critical Infrastructure Protection.
- **Incident Investigation and Analysis Group**
Analysis of targeted e-mails and malware, and investigation of other cyberattack cases.
- **Tokyo 2020 Group**
Promotion of cybersecurity measures for the Tokyo Olympic and Paralympic Games in 2020.

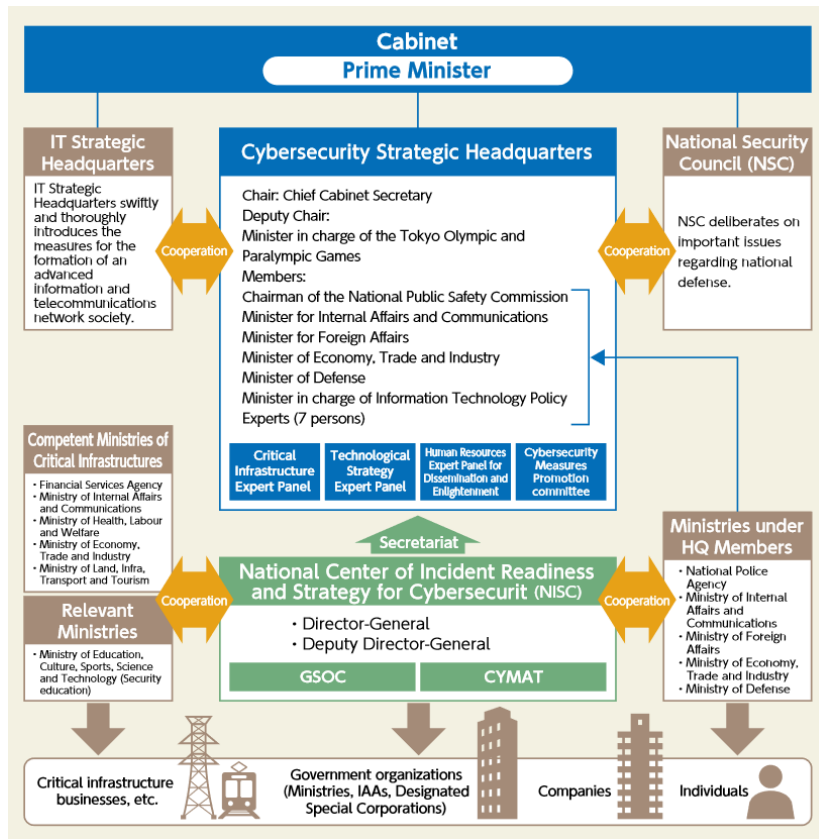


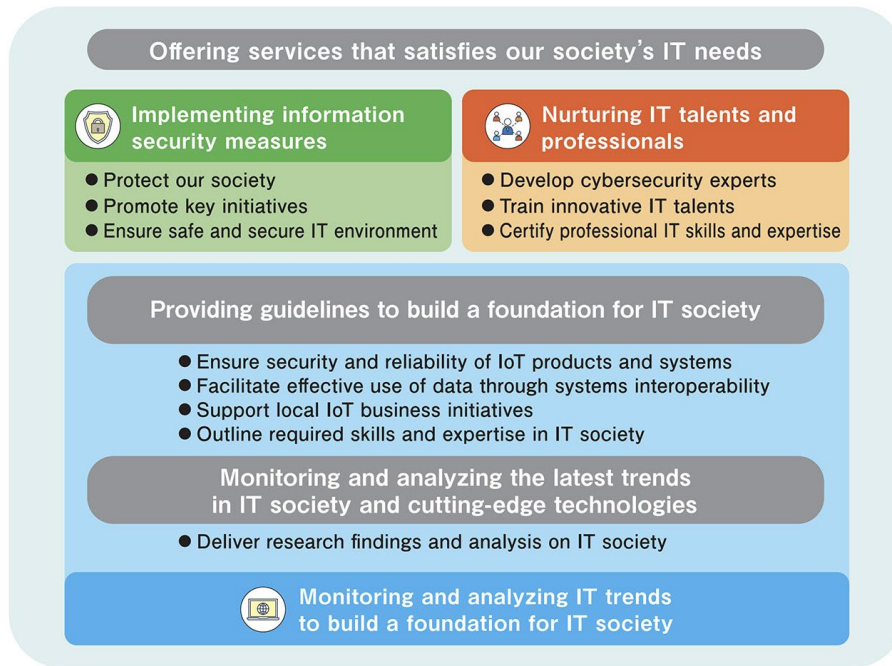
Figure-3 Implementation Framework of NISC¹⁵

2.2.3 IPA (Information-technology Promotion Agency)¹⁶

Established on January 5, 2004, IPA is an Incorporated Administrative Agency that implements various information technology initiatives under the Ministry of Economy, Trade and Industry. The role of IPA is to monitor and analyze IT trends to build the foundation for IT society, and then to implement information security measures as well as to nurture IT talents and professionals. The scope of IPA activities is illustrated in the figure below.

¹⁵ https://www.nisc.go.jp/eng/pdf/Implementation_Framework.pdf

¹⁶ <https://www.ipa.go.jp/>

Figure-4 The Scope of IPA Activities¹⁷

In the cybersecurity field, IPA promotes various initiatives for enterprises and institutions to safeguard their systems and data, engages in activities to raise information security awareness, and encourages the public to implement policies and guidelines for optimal security of IT products and systems. Some of these initiatives are:

- J-CSIP (Initiative for Cybersecurity Information Sharing Partnership of Japan)
- It collects and analyzes data from actual incidents to share findings with participating organizations and industry groups for early detection of attacks and effective countermeasures.
- J-CRAT (Cyber Rescue and Advice Team against Targeted Attack of Japan)¹⁸
- It helps attacked organizations quickly analyze the damage and undertake countermeasures to prevent or reduce further expansion of damage.
- Security risk assessment for industrial control systems
- Security auditing and monitoring for government-affiliated organizations
- Security Action program for SMEs that gives two-tier goals to be achieved
- Leading vulnerability countermeasures promotion initiatives
- Driving information security awareness and promotion initiatives
- JISEC (Japan Information Technology Security Evaluation and Certification Scheme)
- JCMVP (Japan Cryptographic Module Validation Program)
- CRYPTEC (Cryptography Research and Evaluation Committees)

¹⁷ <https://www.ipa.go.jp/files/000058630.pdf>

¹⁸ <https://www.ipa.go.jp/security/J-CRAT/index.html>

2.2.4 NPA (National Police Agency)¹⁹

In Japan, NPA plays an important role for law enforcement regarding cybersecurity²⁰. Not only enforcement, but NPA also implements various activities for the promotion of awareness raising on cybersecurity. NPA has its dedicated division for cybercrime, and it has online cyber police called the “Cyber Police Agency”²¹. There is also “@police”²² which is a website operated by the High-Tech Crime Technology Division of the NPA whose purpose is to prevent cybercrimes and cyber-attacks, and to limit the damage from them.

2.2.5 “Kan-min Board” (Public-Private Board)²³

It is a short name for “Public-private joint committee for opinion aggregation on unauthorized access prevention measures” led by the NPA to gather opinion on the current situation and preventive measures on unauthorized accesses from both public and private sectors. It was established on June 30, 2011, and its members comprise the following organizations and companies.

Table-1 Main Members of the “Kan-min Board”

*	Name	URL
G	NPA (National Police Agency)	https://www.npa.go.jp
G	MIC (Ministry of Internal Affairs and Communications)	https://www.soumu.go.jp
G	METI (Ministry of Economy, Trade and Industry)	https://www.meti.go.jp
G	NISC (National Center of Incident readiness and Strategy for Cybersecurity)	https://www.nisc.go.jp
G	CAA (Consumer Affairs Agency)	https://www.caa.go.jp
G	NICT (National Institute of Information and Communications Technology)	https://www.nict.go.jp
G	AIST (National Institute of Advanced Industrial Science and Technology)	https://www.aist.go.jp
G	IPA (Information-technology Promotion Agency)	https://www.ipa.go.jp
O	JPCERT/CC (Japan Computer Emergency Response Team Coordination Center)	https://www.jpcert.or.jp
I	ISOG-J (Information Security Operation Providers Group Japan)	https://isog-j.org
I	Council of Anti-Phishing Japan	https://www.antiphishing.jp
I	JISA (Japan Information Technology Service Industry Association)	https://www.jisa.or.jp
I	JOGA (Japan Online Game Association)	https://japanonlinegame.org
I	JUAS (Japan Users Association of Information Systems)	https://juas.or.jp
I	EMA (Content Evaluation and Monitoring Association)	http://ema.mcf.or.jp
I	TCA (Telecommunications Carriers Association)	https://www.tca.or.jp
I	JAIPA (Japan Internet Providers Association)	https://www.jaipa.or.jp
I	JCA (Japan Consumer Credit Association)	https://www.j-credit.or.jp
I	JCTA (Japan Cable and Telecommunications Association)	https://www.catv-jcta.jp
I	JNSA (Japan Network Security Association)	https://www.jnsa.org
I	JDCC (Japan Data Center Council)	https://www.jdcc.or.jp
I	TELESA (Telecom Services Association)	https://www.telesa.or.jp

¹⁹ <https://www.npa.go.jp/english/index.html>

²⁰ https://www.jst.go.jp/sicp/ws2010_austria/presentation/presentation_07.pdf

²¹ <https://www.npa.go.jp/cybersecurity/index.html>

²² <https://www.npa.go.jp/cyberpolice/english/index.html>

²³ <https://www.npa.go.jp/cyber/kanminboard/>

*	Name	URL
P	Altair Security Consulting	https://www.altairsecurity.com
P	Check Point Software Technologies Ltd.	https://www.checkpoint.com
P	Hitachi, Ltd.	https://www.hitachi.com
P	IBM Japan, Ltd.	https://www.ibm.com/jp-ja
P	Itochu Techno-Solutions Corporation	https://www.ctc-g.co.jp
P	JCB Co., Ltd.	https://www.jcb.co.jp
P	LAC Corporation	https://www.lac.co.jp
P	McAfee, LLC	https://www.mcafee.com/ja-jp
P	Microsoft Japan	https://www.microsoft.com/ja-jp
P	Hewlett Packard Japan, G.K.	https://www.hpe.com/jp
P	NEC Corporation	https://www.nec.com
P	NTT DATA Corporation	https://www.nttdata.com
P	SCSK Corporation	https://www.scsk.jp
P	SECOM Trust Systems Co., Ltd.	https://www.secomtrust.net
P	Simplex Inc.	https://www.simplex.inc
P	Trend Micro Incorporated	https://www.trendmicro.com
P	Yahoo Japan Corporation	https://www.yahoo.co.jp

* G: Government, O: Organization, I: Industry Association, P: Private Enterprise

2.2.6 GSOC (Government Security Operation Coordination team)

NISC operates a real-time government-wide monitoring team called the Government Security Operation Coordination team (GSOC). It operates the GSOC system designed for cross-government monitoring through sensors installed in each agency, analyzing attacks, providing advice to each agency, promoting mutual collaboration between agencies, and sharing information. The first GSOC team was launched in April 2008 to monitor government agencies, and the second GSOC team started operation in April 2017 to monitor incorporated administrative agencies.

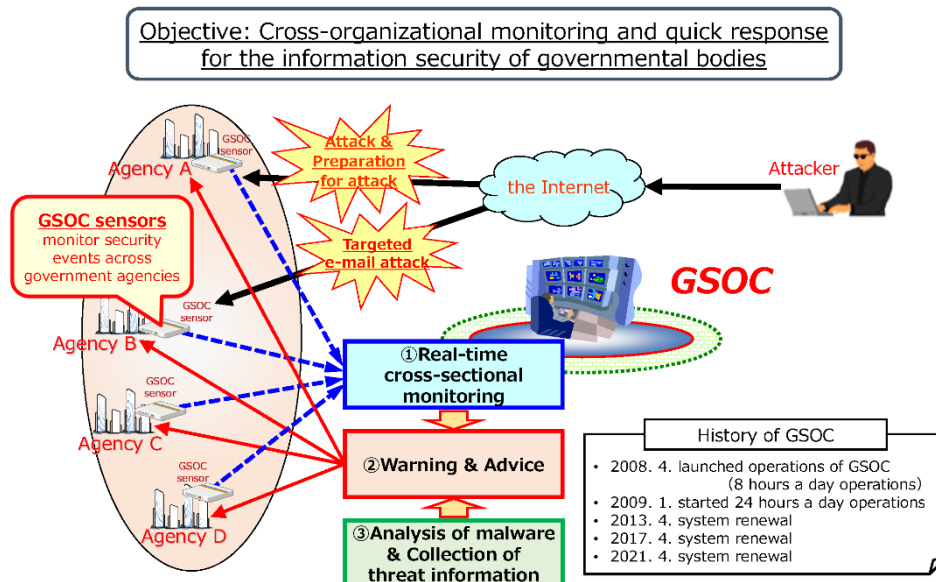


Figure-5 GSOC System Overview²⁴

²⁴ https://www.nisc.go.jp/eng/pdf/211013_GSOC_Overview.pdf

2.3 National Budget on Cybersecurity in Japan²⁵

National budget on cybersecurity (including all activities) in Japan is shown in the figure below.

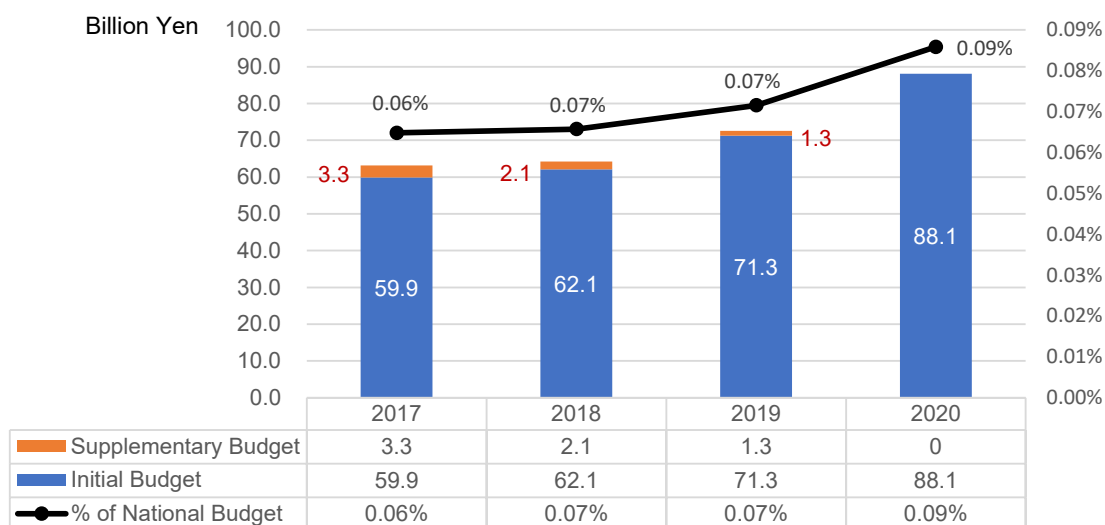


Figure-6 National Budget on Cybersecurity in Japan

In this budget, there is no detailed information on how much budget is allocated to awareness raising activities. But some of the related projects are as follows.

Table-2 Example of Projects related to Awareness Raising

Item	Budget (Billion Yen)	% of Budget on Cybersecurity
Development of Integrated Intelligent Human Resource Development Infrastructure	2.00	2.3%
Enhancement of National Cyber Training Center	1.50	1.7%
Information Sharing Promotion on Cybersecurity	0.36	0.4%

Many awareness raising activities are done through organizations such as IPA, which receives supporting budget from the government: 5.8 billion yen in 2021

²⁵ <https://www.nisc.go.jp/active/kihon/pdf/yosan2017.pdf>
<https://www.nisc.go.jp/active/kihon/pdf/yosan2018.pdf>
<https://www.nisc.go.jp/active/kihon/pdf/yosan2019.pdf>
<https://www.nisc.go.jp/active/kihon/pdf/yosan2020.pdf>

3. Policy, Guideline and Practice regarding Cybersecurity Education in Japan

3.1 Cybersecurity Human Resource Development Program²⁶

Source: NISC **Year:** 2017 **Target:** All **Category:** National program
Format: PDF

This is the national program created by NISC that provides general direction for human resource development for cybersecurity.

(1) Basic policy

- Find appropriate match of the “demand” and “supply” of human resources for cybersecurity
- Clarify career paths for cybersecurity personnel to play an active role under the appropriate recognition
- Human resources should be made available by providing them with solid knowledge and practical skills through education, etc. based on qualifications and evaluation standards.

(2) Target and programs

- Management: Change the mindset to address cybersecurity as a “responsibility” associated with the “challenge” of creating new value.
- Bridge human resources: HR that can plan and develop cybersecurity together with business strategy and lead practitioners.
- Practitioners: Promote cybersecurity as a team work on developing advanced human resources who can realize business innovation with advanced cybersecurity technology expertise

The program indicates that it is important to enhance the information education from the primary and secondary education levels to cultivate the ability to use information (including information security) of students.

3.2 A Guide to the Informatization of Education²⁷

Source: MEXT **Year:** 2020 **Target:** Teachers
Category: Guide **Format:** PDF

This is a guide reference book for teachers developed by MEXT. According to the revised government course (curriculum) guidelines, the “ability to use information” is positioned as a fundamental quality and ability for learning.



²⁶ <https://www.nisc.go.jp/active/kihon/pdf/jinzai2017.pdf>

²⁷ https://www.mext.go.jp/a_menu/shotou/zyouhou/detail/mext_00117.html

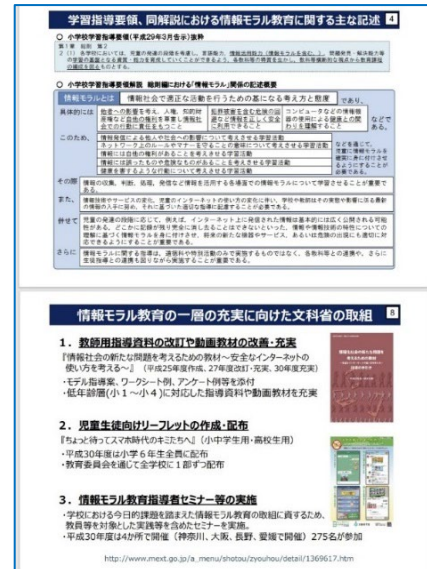
In addition to general guidelines to teach and utilize ICT in education, it covers protective knowledge and skills for cybersecurity.

3.3 Information Moral Education at Schools²⁸

Source: MEXT **Year:** 2019 **Target:** School
Category: Education **Format:** PDF

This document describes principles and activities to promote information moral (and cybersecurity) education at schools. Activities of MEXT in this area are as follows.

- Develop educational materials (including videos) for use in classrooms
- Develop leaflets to promote awareness among children
- Conduct seminars for teachers on information moral education (including basic cybersecurity)
- Promote learning of information morals at home
- Conduct “Net Moral Caravan” in as a symposium for parents
- Cooperation with NPA, MIC, etc.



3.4 Educational Materials for Schools in Japan

There are the following resources on the net regarding educational materials for schools in Japan.

- Leaflets²⁹
- Case studies and materials³⁰
- Videos (69)³¹

4. Human Resources for Awareness Raising in Japan

4.1 Professional Certification in Japan

There are many professional certifications in Japan related to cybersecurity, both domestic certifications and international certifications. These are categorized by their required knowledge / skill levels and their target area as shown in the figure below. Note that all these certifications cover topics on awareness raising to some extent. Some certifications (such as SPREAD in 4.1.3) are more focused on human resources who are in charge of awareness raising activities.

²⁸ https://www.soumu.go.jp/main_content/000662206.pdf

²⁹ https://www.mext.go.jp/a_menu/shotou/zyouhou/detail/1369617.htm

³⁰ https://www.mext.go.jp/a_menu/shotou/zyouhou/detail/1408132.htm

³¹ https://www.youtube.com/playlist?list=PLGpGsGZ3lmbAOd2f-4u_Mx-BCn13GyWDI

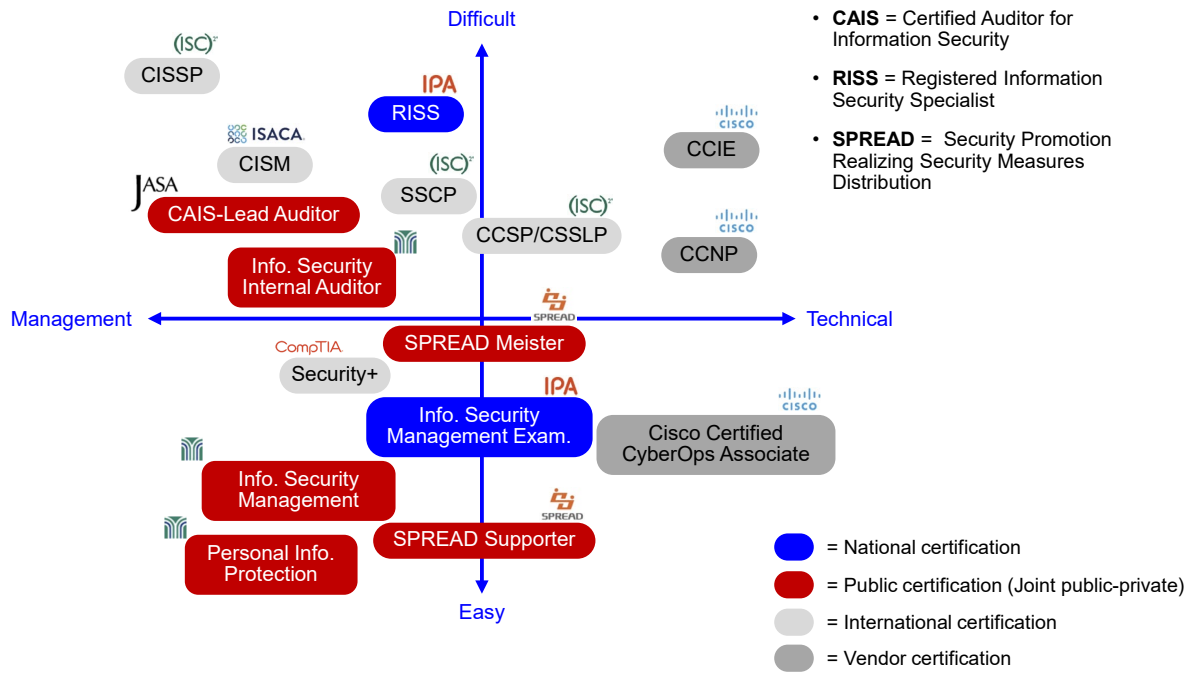


Figure-7 Professional Certifications in Japan related to Cybersecurity³²

Since the information for international/vendor certification is widely available in English on the internet, we focus on major national/public certifications in Japan.

4.1.1 Registered Information Security Specialist (RISS)³³

Source: IPA **Target:** General **Category:** National certification

RISS is a Japanese national certified professional for information security by IPA.

- The most difficult national certification in Japan
 - Former Information Security Specialist exam
- Requires wide range of knowledge and skill in both technological and management areas
 - Network security
 - Database, Programming, Information Systems, etc.
 - IT service management, System audit, Project management, etc.
 - System strategy, Management strategy, Legal, etc.
- Mandatory annual online training/tri-annual group training



³² <https://cybersecurity-jp.com/column/21726>

³³ <https://www.jp-rissa.or.jp/>

4.1.2 CAIS-Auditor³⁴

Source: JASA **Target:** Business **Category:** Public certification

CAIS-Auditor is the most popular information security auditor professional certification in Japan.

- By Japan Information Security Audit Association (JASA)
 - Main members are from big IT companies in Japan
 - Established by the initiative from METI
- There are four levels (steps) of certification, from the highest to lowest:
 - CAIS-Lead Auditor
 - CAIS-Auditor
 - CAIS-Assistant
 - CAIS-Associate



- The certification is primarily targeted at developing dedicated (internal) security auditor in large enterprises.
- JASA also implement awareness raising activities such as seminars and international cooperation.

4.1.3 SPREAD Meister/SPREAD Supporter³⁵

Source: SPREAD **Target:** General **Category:** Public certification

These are certifications issued by SPREAD (Security Promotion Realizing Security Measures Distribution), a council for promotion of security measures in Japan. These certifications are rather easier-to-obtain than other professional certifications.

- Not targeted for independent professionals
 - Rather for promotion of cybersecurity awareness in smaller offices such as SMEs and NPOs
- There are two types of certifications
 - SPREAD Supporter
 - Human resource who can give advice on basic cybersecurity knowledge and measures
 - SPREAD Meister
 - Same as above plus more advanced knowledge on cybersecurity



³⁴ <https://www.jasa.jp/>
³⁵ <https://www.spread.or.jp/>

4.1.4 Information Security Management Examination³⁶

Source: All-Japan Association for the Promotion of Information Learning

Target: General staff **Format:** Public certification

This is a medium-level examination for cybersecurity-related knowledge and skills issued by All-Japan Association for the Promotion of Information Learning.

- Targeted at general staffs in companies/organizations
 - Not technology-oriented, and aimed at promoting “additional” skill & knowledge for general staffs
 - Supported by MEXT
 - The association provides many other kinds of IT-related skill examinations
- Four types of certification for cybersecurity
 - Information Security Internal Auditor
 - Information Security Management
 - Information Security Basics
 - Personal Information Protection



4.2 Non-certification-based Human Resource Development in Japan for Awareness Raising

4.2.1 Cybersecurity Helpers Service Project³⁷

Source: IPA **Target:** SMEs **Category:** Service **Format:** Project

A demonstration project by IPA in 2019/2020 to establish a mechanism to support cybersecurity measures for SMEs, then it was brought into real implementation in 2021.

- Focusing on post-incident measures to be conducted in a self-assisted manner
- Created a logo for the compliance to “Cybersecurity Helpers Service Standard”
- IPA provides support for SMEs to introduce the standard
- Adopted by SMEs and local chamber of commerce in Japan

(1) Overview of Cybersecurity Helpers Service

This project was first initiated by IPA, and it implemented PoC (Proof of Concept) programs in 2019 and 2020. Based on the result of two years of PoC programs, METI and IPA officially

³⁶ <https://www.joho-gakushu.or.jp/isme/>

³⁷ <https://www.ipa.go.jp/security/keihatsu/sme/otasuketai/index.html>

launched the mechanism to certify and register the Cybersecurity Helpers (by private sector) in 2021. The figure below illustrates the overall picture of this project.

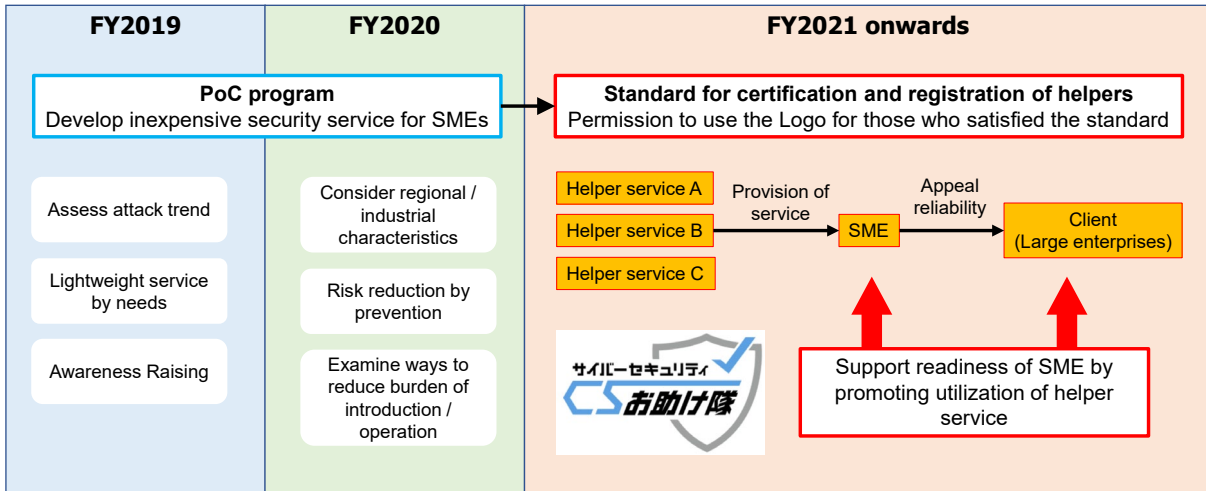


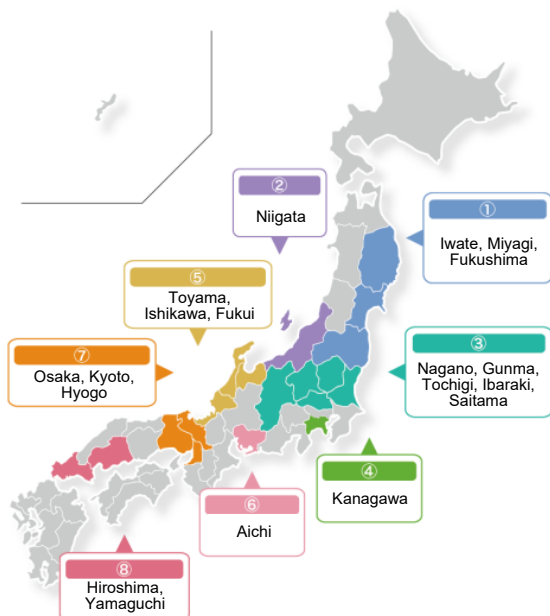
Figure-8 Overall Picture of Cybersecurity Helpers Project³⁸

(2) PoC program implemented in FY2019³⁹

The first PoC was conducted in FY2019 in eight regions of Japan, by 1,064 participating SMEs in total. As a result, 128 incident supports were made during the PoC with 18 on-site services.

<PoC area>

8 region (19 prefectures)



<Concept of PoC>

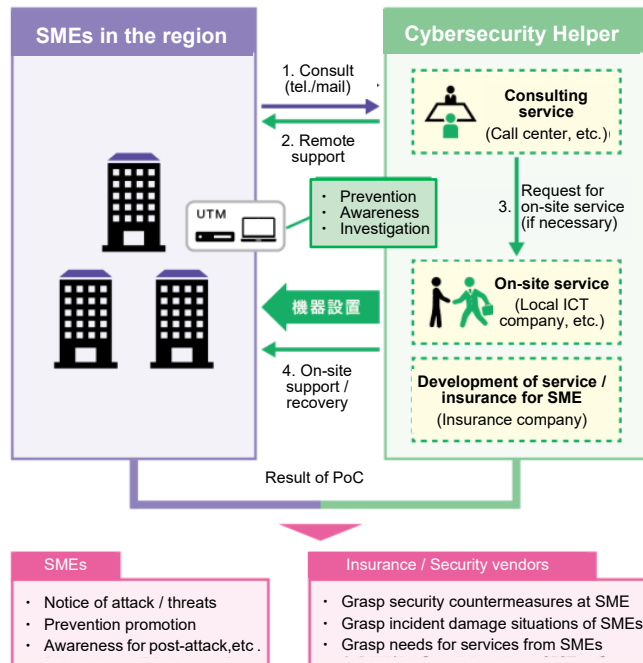


Figure-9 Target Area and the Concept of Cybersecurity Helpers PoC in 2019

³⁸ <https://www.cyber-otasuke.jp/>

³⁹ https://www.ipa.go.jp/security/fy2019/reports/sme/otasuketai_houkoku.html

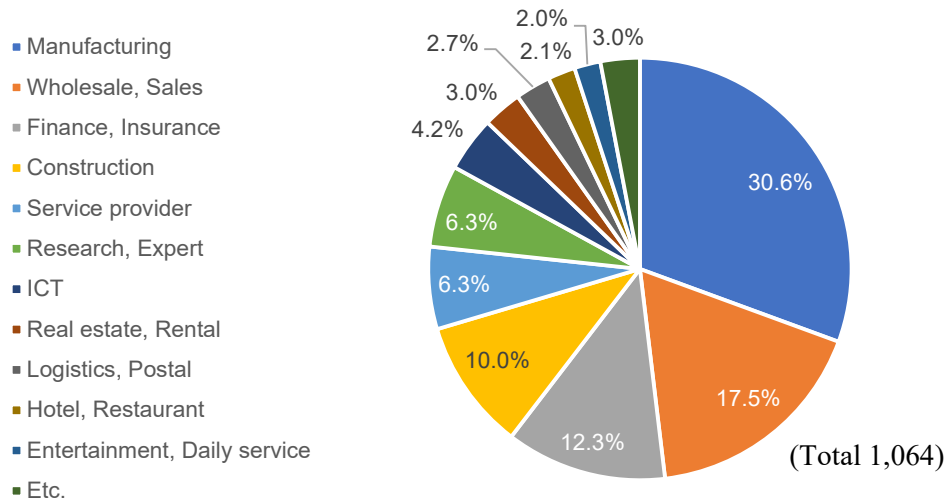


Figure-10 SMEs Participation by industry for Cybersecurity Helpers PoC (2019)

(3) PoC program implemented in FY2020⁴⁰

In 2020, based on the results of the 2019 program, IPA tried to study regional and industrial characteristics, and promoted studies to streamline the service content and reduce the introduction and operation cost in order to start real services in the private sector.

Similar to the FY2019 project, this demonstration project was also exposed to the threat of cyber-attacks regardless of industry or scale, and it has become clear that existing measures such as antivirus software cannot prevent it. In addition, some vulnerabilities (weaknesses) were found in most of the target companies in the vulnerability diagnosis of homepages and service sites published on the Internet. In addition, approximately 20% of the companies were diagnosed as having the potential to lead to serious incidents.

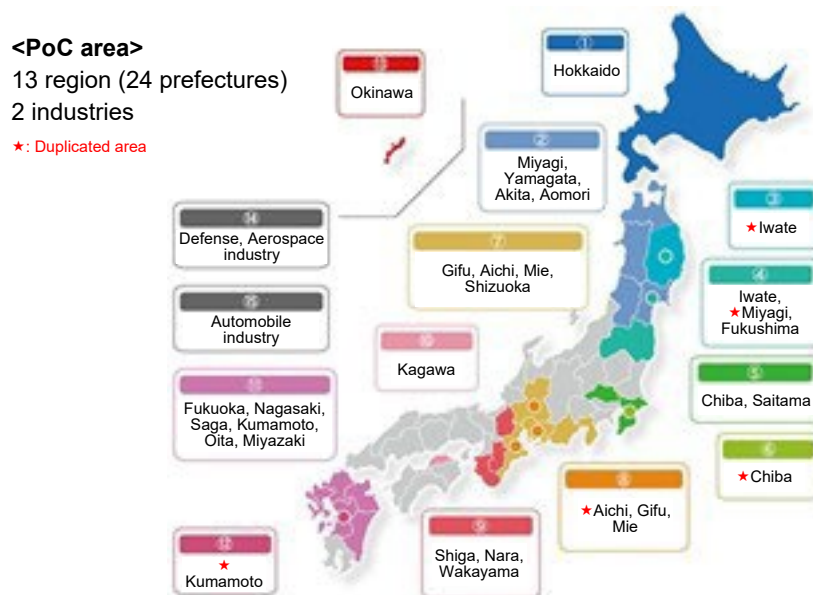


Figure-11 Target Areas of Cybersecurity Helpers PoC in 2020

⁴⁰ https://www.ipa.go.jp/security/fy2020/reports/sme/otasuketai_houkoku.html

(4) Real service started in FY2021⁴¹

The Cybersecurity Helper Service mechanism officially started in 2021. In this mechanism, a service provider must comply with the following two standards.

- Service standard⁴²
- Certification and registration standard⁴³

IPA accepts application for becoming the Cybersecurity Helper Service Provider⁴⁴ (around two times per year), then will check the applicants for the above standards and allow them to use the logo if they pass.



Figure-12 Logo of the Cybersecurity Helpers

4.2.2 Education Committee, Japan Network Security Association⁴⁵

Source: JNSA **Target:** Teachers **Category:** Organization **Format:** Web

This is a working group in JNSA dedicated to education on cybersecurity. It has the following activities.

- Study on required knowledge and skills on cybersecurity
- Evaluate experiments conducted at universities and vocational schools
- Develop lecture syllabus and materials for education
- Develop SecBoK⁴⁶
- Cooperate with overseas educational institutions mainly in ASEAN
- Conduct seminars for lecturers, maintaining database of lecturers, etc.



⁴¹ <https://www.ipa.go.jp/security/otasuketai-pr/>
⁴² <https://www.ipa.go.jp/files/000092713.pdf>
⁴³ <https://www.ipa.go.jp/files/000088837.pdf>
⁴⁴ <https://www.jnsa.org/sme/otasuketai/>
⁴⁵ <https://www.jnsa.org/active/2021/edu.html>
⁴⁶ <https://www.jnsa.org/result/skillmap/>

4.2.3 Prefecture-level Activities for Cybersecurity Awareness

There are many joint efforts of local government, local police, and local industries on awareness raising activities of cybersecurity in Japan. Some examples are given below.

- Saitama Prefecture Computer Network Crime Prevention Liaison Council⁴⁷
 - Provides seminars, research, etc.
- Kagawa Prefecture Cybersecurity Liaison Network⁴⁸
 - Information sharing, Awareness raising, HR development, etc.
- Fukuoka Prefecture Information Security Liaison Council⁴⁹
 - Cybercrime prevention, information sharing, etc.

5. Overview of awareness raising activities in Japan

According to the “Cybersecurity Awareness and Action Enhancement Program” (→ 9.1.2), there are the following awareness raising activities in Japan as of 2019.

⁴⁷ <http://www.saitama-cn.gr.jp/index.html>

⁴⁸ <https://www.e-topia-kagawa.jp/cyber-security/network.html>

⁴⁹ https://www.police.pref.fukuoka.jp/seian/cyber/sesaku_torikumi/029.html

5.1 Public Seminars on Cybersecurity Awareness Raising

Target (Individual)			Target (Organization)					
Young / Children	Working generation	Elderly people	Inhouse / self-employed	SME	Large Enterprises	Educational institutions	Local Government	
Cybersecurity month event (NISC)			Regional events (NPA, Regional Police)					☐ = Public sector
Seminars related to cybersecurity (MIC, etc.)			Promotion of digital signature and trust services (MIC, MOJ, METI)					
Net Moral Caravan (MEXT)			Dispatch of lecturers to SME supporting organizations (METI, IPA)					
"Let's Expand Information Morality and Security" Competition (METI, IPA)			Seminar on lecture capacity development (METI, IPA)					
Promotion of info. morality education (MEXT)			Info. sharing by JPCERT/CC (METI)					Internet safety class (METI, IPA, JNSA)
Training for teachers (NITS, MEXT)			Seminar on phishing prevention (METI, CAPJ, JPCERT/CC)					
Internet safety class (METI, IPA)			HR development and awareness raising on cybersecurity in Kansai (METI Kansai, MIC Kansai, KIIS)					
e-Net caravan (FMMC, MIC, MEXT)								

5.2 Private Seminars on Cybersecurity Awareness Raising

Target (Individual)			Target (Organization)				
Young / Children	Working generation	Elderly people	Inhouse / self-employed	SME	Large Enterprises	Educational institutions	Local Government
	Slogan contest (FMMC, MIC, MEXT)		Seminars, trainings, study sessions, practices (JASA)				
	Development of info. security Meister, Meeting (SPREAD)		JC3 forum (JC3)				JC3 forum (JC3)
	Grassroot cybersecurity movement conference (Grafsec)				Seminars / announcement for top management (Keidanren)		
	Study sessions by regional organizations (supported by Grafsec)				Top management meeting (CRIC CSF)		
	Seminars, events, contests (JNSA)						
Seminars for students (CRIC CSF)			Control systems security conference (JPCERT/CC)				
							<div style="border: 1px solid black; width: 15px; height: 10px; display: inline-block; vertical-align: middle;"></div> = Private sector

5.3 Tools and Contents on Cybersecurity Awareness Raising

Target (Individual)			Target (Organization)				
Young / Children	Working generation	Elderly people	Inhouse / self-employed	SME	Large Enterprises	Educational institutions	Local Government
Info. security handbook (NISC)			Operation of security presenter (METI, IPA)				
Concise manual for Wi-Fi users (MIC)			Security handbook for Wi-Fi providers (MIC)				
Provisions of tool for information leakage prevention (METI, IPA)							
Info. morality education (MEXT)			<ul style="list-style-type: none"> • Web for supporting info. security • Cybersecurity guideline for SME • Security Action (METI, IPA) 				
Awareness raising videos / leaflets (JISPA)			Self-checker for cybersecurity understanding (JNSA)				
Teaching materials (SPREAD)			Cybersecurity education game (JNSA)				
Self-checker of understandings (JNSA)			Cybersecurity management guideline, Cloud security audit supporting tool (JASA)				
Cybersecurity education game (JNSA)			Cybersecurity training database (CRIC CSF)				
Cybersecurity training database (CRIC CSF)			<ul style="list-style-type: none"> • Security control room kit • HR definition reference (CRIC CSF) 				
			Security first step for introducing industrial IoT (JPCERT/CC)				

5.4 Information Dissemination/Consultation Service

Target (Individual)			Target (Organization)				
Young / Children	Working generation	Elderly people	Inhouse / self-employed	SME	Large Enterprises	Educational institutions	Local Government
Information dissemination by SNS (NISC)							
Consultation service for cyber crime (Prefectural police)							
@police (NPA)							
Cyber crime prevention site (NPA)			Special consultation service for targeted attack / Cyber rescue team (J-CRAT) (METI, IPA)				
Info. security consultation service (METI, IPA)			"Security Action" email news (METI, IPA)				
			SME support network (Tcyss, etc.)				
Alert, announcement to user of vulnerable IoT devices to cyber attack (MIC, NICT, Telecom operators)							
Information dissemination by Web, Blog (SPREAD)			Incident response (JPCERT/CC)				
			Early warning information (JPCERT/CC)				
			Information dissemination by Web, SNS, Mail magazine (JNSA)				

6. Materials for Cybersecurity Awareness Raising in Japan

6.1 Web Portals/Information sites/Web Services

6.1.1 Information Security Portal site “Start here for security!”⁵⁰

Source: IPA **Target:** General **Category:** Portal site **Format:** Web

This is the biggest online portal site for cybersecurity awareness raising in Japan. The site is hosted by IPA, and the contents are provided by “Kan-min Board” (Public-private Board) which is a group of related public and private organizations. It contains wide variety of information links divided into many categories.

- There are links to many educational materials and information produced by the public and private sectors (for the general public and for businesses).
- Target wise:
For elementary school students (13 items),
For middle and high school students (78 items),
For home users (223 items)
- Special features:
For New Employees (13 items),
Telework (37 items),
For SMEs (36 items),
For Managers (44 items),
For General Employees and Staff (36 items),
For System Administrators (45 items)



6.1.2 Information Security Site for People/for Kids⁵¹

Source: MIC **Target:** General **Category:** Information. site **Format:** Web

These web sites contain fundamental knowledge and information on cybersecurity for general public.

- Basic knowledge
- Countermeasures for general users
- Countermeasures for companies and organizations

There is also a version for kids

- Provides easy to understand explanation on cybersecurity, threats and countermeasures



⁵⁰ <https://www.ipa.go.jp/security/kokokara/>

⁵¹ https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/

6.1.3 Is your child safe? Beware of smartphones! The pitfalls of online crime.⁵²

Source: Government of Japan Public Relations Online **Target:** Parents
Category: Info. site **Format:** Web

This website contains information for parents regarding smartphone-related cybercrimes such as the followings.

- Increasing cases of child victim of net crime
- What kinds of cybercrimes are there?
- Cases where kids becomes offender, not victim
- How to use the internet safely and appropriately
- Have you applied filtering to your children?
- Examples of internet usage rules at home
- Consulting service is available nationwide



6.1.4 Internet Dangers and Security to Remember with kids⁵³

Source: JAO **Target:** Parents **Category:** Information site **Format:** Web

This is a concise webpage to learn threats and countermeasures of internet usage for parents, designed for learning with their children. Topics covered in the site are:

- Danger of using the internet
 - SNS, Adult sites, BBS, Malware, etc. (15 topics)
 - Countermeasures
 - Update OS, Security tool, etc. (5 topics)
 - Things that you should discuss with your children
 - Manner, Personal info, etc. (10 topics)



⁵² <https://www.gov-online.go.jp/useful/article/201503/3.html>

⁵³ <https://thehikaku.net/security/danger/child.html>

6.1.5 Useful Web for School Information Security⁵⁴

Source: ISEN **Target:** Teachers **Category:** Information site **Format:** Web

This is a dedicated website for safety and cybersecurity at school that contains useful information for promoting ICT utilization at schools and for preparation of cybersecurity such as the followings.

- News, statistics, and reports on security incidents at schools
- Tips for cybersecurity
- Free clip arts and teaching materials for cybersecurity education



6.1.6 NPO Information Security Forum⁵⁵

Source: NPO Information Security Forum **Target:** Teachers **Category:** Links **Format:** Web

This website contains a comprehensive list of links to surveys, reports, and teaching materials on cybersecurity education. The information in the site is searchable by such topics as follows:

- Malware, Smartphone, website, Cybersecurity measure at school, Teaching materials, etc.
- Searchable by target parties:
- Teachers, Elementary students, Secondary students, High-school students, Parents, etc.



⁵⁴ <https://school-security.jp/>

⁵⁵ <https://www.isef.or.jp/sci/index.html>

6.1.7 Free! Educational Materials and Countermeasures Guide for Information Security⁵⁶

Source: ISM **Year:** 2019 **Target:** Teachers **Category:** Links
Format: Web

It contains a list of links to freely available teaching materials for cybersecurity education. There are the following number of links contained in the site.

- Awareness Raising (1)
- Learning materials (7)
- Training materials (2)
- Manual, Guidebook (10)
- Self-checking tools (3)



6.2 Textbooks/Materials

6.2.1 Information Security White Paper⁵⁷

Source: IPA **Target:** General **Category:** White paper **Format:** PDF

This is the annual white paper issued by IPA that contains detailed information about cybersecurity trends such as the following.

- Current trend of security incidents and vulnerabilities
- Current situation of information security policies, human resource development, countermeasures, standards, etc. in Japan and the world
- Selected topics for the year (in 2021 edition)
 - Cybersecurity of controlling system
 - Cybersecurity of IoT
 - Cybersecurity of telework
 - Activities of NIST



⁵⁶ <https://www.ismwebstore.com/materials/archives/3146>

⁵⁷ <https://www.ipa.go.jp/security/publications/hakusyo/2021.html>

6.2.2 White Paper on Information and Communication Technology⁵⁸

Source: MIC **Target:** General **Category:** White paper **Format:** PDF

This is the annual white paper issued by MIC that contains a wide range of ICT situations in Japan. The latest edition (2021) has the following contents:

- Current situation and issues of digitalization
- Accelerated digitalization due to COVID-19
- Digitalization and SDGs
- Basic data on ICT
- Trend in ICT policy

There are also some topics related to cybersecurity such as “Security risk of telework due to COVID-19”



6.2.3 10 Major Security Threats 2021⁵⁹

Source: IPA **Year:** 2021 **Target:** General

Category: Awareness raising **Format:** PDF

This is the annual report and awareness raising material for 10 major security threats observed in Japan. The latest issue (2021) has the ranking of 10 major threats as shown in Table-3. English version is also available for enterprise threats⁶⁰.



Table-3 10 Major Security Threats of 2021

For individuals	Rank	For enterprises
Fraudulent Use of Smartphone Payment	1	Ransomware Attacks
Phishing Fraud for Personal Information	2	Confidential Information Theft by APT
Cyberbullying and Fake News	3	Attacks on New Normal Work Styles such as Teleworking
Extortion of Money by Blackmail, etc.	4	Attacks Exploiting Supply Chain Weaknesses
Fraudulent Use of Leaked Credit Card Information	5	Financial Loss by Business E-mail Compromise
Unauthorized Use of Internet Banking Credentials	6	Information Leakage by Internal Fraudulent Acts
Personal Information Theft from Services on the Internet	7	Suspension of Business due to Unexpected IT Infrastructure Failure
Internet Fraud by Fake Warnings	8	Unauthorized Login to Services on the Internet
Malicious Smartphone Applications	9	Unintentional/Accidental Information Leakage
Unauthorized Login to Services on the Internet	10	Increase in Exploitations following the Release of Vulnerability Countermeasure Information

⁵⁸ <https://www.soumu.go.jp/johotsusintokei/whitepaper/>

⁵⁹ <https://www.ipa.go.jp/security/vuln/10threats2021.html>

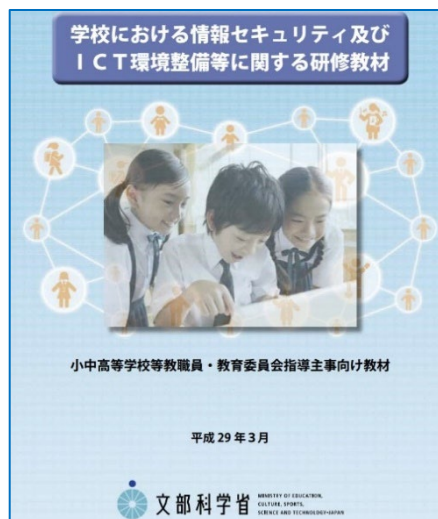
⁶⁰ <https://www.ipa.go.jp/files/000092855.pdf>

6.2.4 Training Materials on Information Security and ICT Environment Maintenance in Schools⁶¹

Source: MEXT **Year:** 2017 **Target:** Teachers
Category: Training materials **Format:** PDF

This is the training material for teachers of elementary /secondary/high schools as well as for staffs in charge of ICT systems at the board of education in each prefecture/city. The contents of the training material for teachers are:

- Guideline for utilizing of ICT in education
- Information security required in schools
- For staff in charge of information systems at education board /maintenance service providers (Part 1/2)
- Same content as above with much more technical details
- Each version contains guidelines and many checklists for regular information security

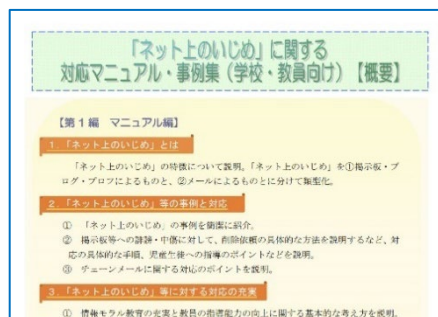


6.2.5 Response Manual and Case Studies on “Cyber Bullying”⁶²

Source: MEXT **Year:** 2008 **Target:** Teachers **Category:** Manual **Format:** PDF

This is a manual for teachers to help them understand and respond to child bullying on the net. It consists of two parts.

- Part 1: Manual
 - What is “bullying on the net”?
 - Typical cases and their appropriate responses
 - How to cope with various cases
- Part 2: Case studies
 - 15 detailed cases in elementary school, secondary school, and high school



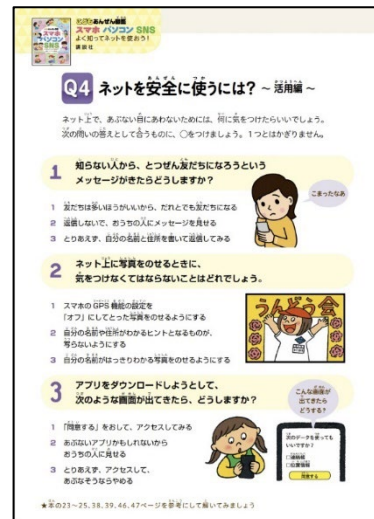
⁶¹ https://www.mext.go.jp/a_menu/shotou/zyouhou/detail/1403475.htm

⁶² https://www.mext.go.jp/b_menu/houdou/20/11/08111701/001.pdf

6.2.6 Kodomo Anzen Zukan: Smartphone, PC, SNS⁶³

Source: Koudansha **Target:** Kids **Category:** Encyclopedia **Format:** Book

This book is an encyclopedia for children about safe use of smartphone/PC/SNS. The content is full color pages and has easy-to-understand explanations using cartoons, photos, and charts.



6.2.7 Let's Think Safe Usage of SNS!⁶⁴

Source: Kanagawa Prefectural Police **Year:** 2021 **Target:** Kids
Category: Teaching materials **Format:** PDF

This is a set of free teaching materials for safe SNS usage designed for teachers and students of elementary/secondary schools. There are the following contents available for free download.

⁶³ <http://ehon.kodansha.co.jp/anzen>

⁶⁴ <https://www.police.pref.kanagawa.jp/mes/mesd5053.htm>

- Slides for teachers to be used in the classroom
- Guidebook for teachers how to teach the content
- Worksheets for students

Topics covered in the contents are:

- Think difference between the opponent and me
- Think information of the opponent
- Think good message delivery
- Think information derived from photos
- Think safe way to send photos
- Think countermeasures to troubles
- Think minimizing the damage



6.3 Manga/Cartoons

6.3.1 Our Smartphone Lives⁶⁵

Source: IPA **Target:** Office workers **Category:** Awareness raising

A manga series for raising awareness of safe usage of smartphone at office. Designed to be viewed on smartphone screen, but PDF version is also available.

Episodes are as follows.

1. Don't look at so much!
2. Hidden truth of convenient apps
3. Wait for that installation!
4. Take good care of apps!
5. Watch carefully!
6. Everyone is watching you!



6.3.2 Understanding 5 Phishing Prevention Measures⁶⁶

Source: Council of Anti-Phishing Japan **Target:** General **Category:** Awareness raising

A manga (cartoon) to explain five typical cases of phishing and their prevention measures. The target of the material is the young generation, but it can also be used by adults who have no or little knowledge about phishing. Episodes are as follows.



⁶⁵ https://www.ipa.go.jp/security/keihatsu/love_smartphone_life/comics/index.html

⁶⁶ <https://www.antiphishing.jp/phishing-5articles.html>

1. Risky if not the latest?
2. Missing suspicious emails?
3. Impersonated email links?
4. Report if you find suspicious matters
5. Real preparedness for digital traps

6.3.3 Learning Security Management by Manga for SMEs⁶⁷

Source: EnterpriseZin **Target:** SMEs **Category:** Security Management

A manga for SMEs to learn cybersecurity management in the office. It conveys the importance of security management and IT assets management as well as personal information management.



6.3.4 Introduction to Security for First-time Smartphone Users⁶⁸

Source: Google **Target:** Young
Category: Awareness

A manga (cartoon) featuring a young boy about to start surfing on the internet by using smartphone for the first time.

(Synopsis): He encounters troubles such as password leakage and phishing fraud, but with the help of advice from his friend, he overcome those troubles.



6.3.5 IT Passport Exam Preparation Episode 3 “Beware of phishing!”⁶⁹

Source: IPA **Target:** General **Category:** Awareness

This material is prepared by IPA for the promotion of its “IT passport” certification examination by using manga. There are three episodes, the third of which is for the prevention of phishing. The targets are new employees of private companies who start using PCs for their work. The implication of the material is that this knowledge for prevention is a part of IT passport certification which covers all fundamental necessary knowledge and skills for using IT in daily work.



⁶⁷ <https://enterprisezine.jp/iti/detail/3423>
⁶⁸ <https://www.google.co.jp/events/webrangers/comic.html>
⁶⁹ <https://www3.jitec.ipa.go.jp/JitesCbt/html/uemine/profile.html>

6.4 Videos/Animations

6.4.1 Awareness Raising Videos by IPA⁷⁰

Source: IPA **Target:** General **Category:** Awareness raising

IPA has its own YouTube channel⁷¹, and it provides nearly 750 videos in various topics. Of these, there are nearly 40 videos related to cybersecurity awareness raising targeted to companies, children, and general public.

Several tables below show the lists of these videos and animations. Note that “Video ID” column indicates YouTube Video ID that you can watch by specifying it in the URL like shown below.

<https://www.youtube.com/watch?v=ID>



Table-4 Short Animation Series “Cybersecurity Helpers Service” by IPA (2021)⁷²

No.	Title	Topic	Target	Video ID
1	Cybersecurity Helpers Service THE MOVIE	Promotion	SME	Xdkvv2J4sMQ
2	Ransomware	Promotion	SME	fk5gx8As1PU
3	Malwares	Promotion	SME	QY11hZ7WL64
4	Incautious software downloading	Promotion	SME	H-aIVehOu70

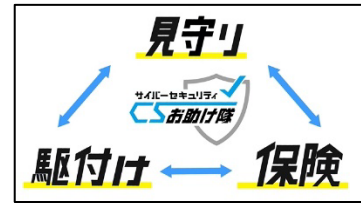


Table-5 Short Animation Series “Let’s learn cybersecurity basics with piglet” by IPA (2020)⁷³

No.	Title	Topic	Target	Video ID
1	Vulnerability Countermeasures	System Update	general	kX-Khx00e2I
2	Computer Virus Countermeasures	Antivirus	general	wY8Ev5LCyrs
3	Unauthorized Access Countermeasures	Good Password	general	Btk6K4Tk7eQ
4	Review Configurations	Safe Configuration	general	numsevf1cGg
5	Know the Threat Tactics	Anti-Phishing	general	pvGDKWm33F8

⁷⁰ <https://www.ipa.go.jp/security/keihatsu/videos/index.html>

⁷¹ <https://www.youtube.com/user/ipajp/videos>

⁷² https://www.youtube.com/playlist?list=PLi57U_f9scILMkVG4pJrAxhZXD2ksBNs-

⁷³ https://www.youtube.com/playlist?list=PLi57U_f9scILMkVG4pJrAxhZXD2ksBNs-



Table-6 Short Video Series “Fraud Technique Verification” by IPA (2021)⁷⁴

No.	Title	Topic	Target	Video ID
1	Install apps from fake security alerts	Threats Demo	general	-CsY92PkHEo
2	Fake absence notification SMS (Android)	Threats Demo	general	28z5Ys03TfY
3	Fake absence notification SMS (iPhone)	Threats Demo	general	THsrXjE08AY
4	iPhone calendar spam	Threats Demo	general	cLLiLy1NwWc
5	Facebook messenger spam	Threats Demo	general	8Iwes88NiNM
6	Fake security warning	Threats Demo	general	SP00wbawM1k
7	Fake browser notification for smartphones	Threats Demo	general	fp_ne7GC6SA
8	Fake browser notification PC	Threats Demo	general	7YoWcoZkTPM
9	Fake sextortion email	Threats Demo	general	p5_arhT6Bgo

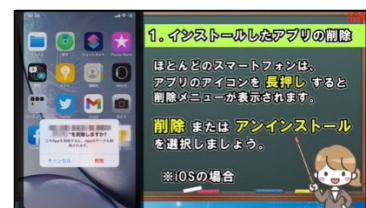
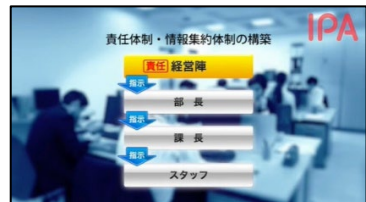


Table-7 Short Video Series “Targeted Cyberattack” by IPA (2012~2016)

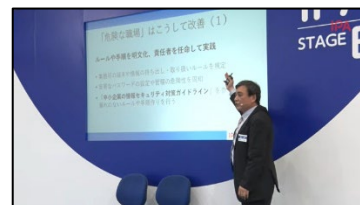
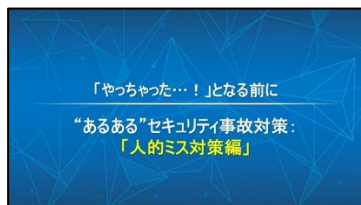
No.	Title	Topic	Target	Video ID
1	Protect your organization's information assets! - Management for targeted cyberattacks-	Targeted Cyberattack	office	q1cIBH1UKd0
2	Invisible Cyber Attacks -Organized Countermeasures for Targeted Cyberattacks-	Targeted Cyberattack	office	ZZJ7VMJ5Btw
3	Can I really trust the email? -Methods and countermeasures for targeted cyberattack emails-	Targeted Cyberattack	office	5K9U0-ASQM8
4	Get to know the demo! Threats and countermeasures for computer hijacking due to targeted attacks	Targeted Cyberattack	office	dSWrKh5FHKA
5	The virus is aimed at your business and your private life!	Targeted Cyberattack	office	2ek0_-VCHhQ
6	Your organization is targeted! -Targeted attacks: The threats and countermeasures-	Targeted Cyberattack	office	NTOF4XcI8j0



⁷⁴ https://www.youtube.com/playlist?list=PLi57U_f9scILMkVG4pJrAxhZXD2ksBNs-

Table-8 Short Video Series “Skits - Learn before suffering from security incidents” by IPA (2019)

No.	Title	Topic	Target	Video ID
1	Countermeasures for Human Error	Security incidents	office	zEXyWQsj6q0
2	Inexpensive countermeasures	Security incidents	office	jeeBZ4XtXCs

Table-9 Other videos and animations for awareness raising by IPA⁷⁵

No.	Title	Topic	Target	Video ID
1	Information Security in Southeast Asia-Current Situation and Countermeasures-	Information	enterprise	xdgg_5aZ9hM
2	Which one are you? -Correct usage of PCs, mobile phones and smartphones-	Ethics	general	k2VT6x4wBSk
3	Three Bags-The Threat of Information Leakage for New Employees-	Ethics	office	F1jLaQA-cRU
4	Is it okay to believe that warning message? Beware of "fake warnings" in your browser!	Phishing	general	sm1UMc97zRc
5	Control systems are also being targeted now! -Necessity of information security-	Infrastructure	enterprise	NdMs45qBtbA
6	Get to know the demo! Threats and countermeasures for smartphone hijacking	Hijacking	general	7erVwpc1100
7	Is your password okay? -Countermeasures against unauthorized login of Internet services-	Password	general	1Xh0b4KS9gE
8	Your writing is seen all over the world -knowing how to use SNS properly-	SNS	general	tvZSuGkmnGQ
9	Your home is also targeted !? Internet home appliance security measures taught by a tutor!	Home appliance	home	xbn8SZIib90
10	Inspection! One-click billing for smartphones	Phishing	general	f7DbLwEGX-Q
11	Hidamari Family and Password- Three Points to Protect Yourself-	Password	home	3afaAbFUK4g
12	Temporary staff solved it! Key points for creating information security regulations	Regulations	office	fot-PEzBZ04
13	Your smartphone, virus is aiming! -Security measures for smartphones and tablets-	Malware	general	0mUetZGyXUs
14	Nice to meet you, this is Peaco. -Promises for parents and children's smartphones-	Ethics	family	xvgBJFudoMs
15	Real security story			b61e7CTr-ak
16	Your Company's Security Doctor -Basics of Information Security Measures for SMEs-	Basics	SME	OP7012w6KnQ
17	The danger of hijacking is also on your smartphone! -Security measures for smartphones and tablets-	Hijacking	general	_XiBB42q9z8
18	Let's know the trap of one-click billing! -Sophisticated techniques and countermeasures-	Phishing	general	8VHBkZi9sHg
19	Message from my wife -Telework security-	Telework	home	zDs88SLymwo
20	Who leaked the information? -Countermeasures against internal fraud and information leakage-	Leakage	office	5Z_10h2aA8c
21	Is your smartphone OK? -Security measures for security and safety-	Smartphone	general	AhiUC7X3VSg

⁷⁵ https://www.youtube.com/playlist?list=PLi57U_f9scILMkVG4pJrAxxZXD2ksBNs-

6.4.2 Awareness Raising Videos by National Police Agency⁷⁶

Source: NPA **Target:** General **Category:** Awareness raising

NPA has its own YouTube channel, and it provides nearly 400 videos in various topics. Of these, there are nearly 100 videos related to cybersecurity. Most of them are for awareness raising purposes such as the following.

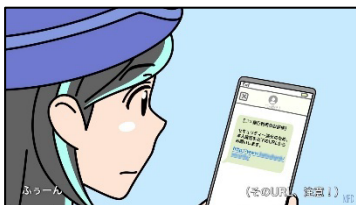
- Short animation series (16) for cybercrime prevention
- Short video series (5) for senior citizens for cybercrime prevention
- Short video series (6) “Threats in cyberspace – Now your company is targeted –”
- Short video series (6) for youth awareness raising



Several tables below show the lists of these videos and animations.

Table-10 Short Animation Series for Cybercrime Prevention by NPA (2019~)

No.	Title	Topic	Target	Video ID
1	Fake live broadcasting	Phishing	young~adult	dY7GfypCC0k
2	IoT device hijacking	Hijacking	family	0epAjVudSUo
3	SMS from fake financial institution (bank)	Phishing	general	1WvStEystrg
4	Wi-Fi free spots are not safe	Eavesdropping	general	HRqBdDRf4_c
5	Fake online shopping site	Phishing	general	6Jj37AjoXjk
6	Unattended QR code theft	Info theft	general	cNZfM23A44c
7	Phishing lead to fake site	Phishing	general	Fhre4eKE2es
8	Fake virus alert	Phishing	general	sTf-1IKUGQE
9	Spoofing email with malicious attachment	Spoofing	office	rW182-eI9Yw
10	Targeted threat	Spoofing	office	f1cWLiZT3_U
11	Mobile app claiming unnecessary permissions	Malware	general	Jb_r5Q1JmNg
12	For those who use smartphone for the first time	Phishing	Aged people	T6yFJefqz1U
13	Ransomware	Ransomware	office	9oUJrDnp09A
14	Security for work from home/telework	Vulnerability	office	IBXKD1xbPRg
15	Phishing lead to very realistic fake site	Phishing	general	BsC574MbmHA
16	Supply chain attack	Phishing	office	tMGoOWLWh-A



⁷⁶ <https://www.youtube.com/channel/UC1VghyKU1Nb-Gs8Hv1xmaJw/videos>

Table-11 Short Video Series Aimed at Senior Citizens for Cybercrime Prevention by NPA (2019~)

No.	Title	Topic	Target	Video ID
1	Undelivered parcel notice by email	Phishing	Senior citizen	fvPwRSXnvxE
2	Fake virus alert	Phishing	Senior citizen	oTgf80XJCZ8
3	Email asking personal information from bank	Phishing	Senior citizen	lpZpBHzB45M
4	Demanding registration fee on smartphone	Phishing	Senior citizen	hnYjr0tF2vA
5	Fake 80% off sale on fake shopping site	Phishing	Senior citizen	RXGhhpmIKM

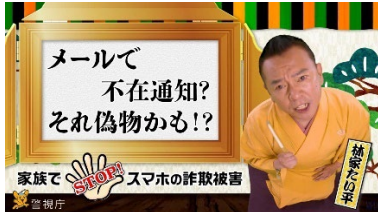


Table-12 Short Video Series “Threats in cyberspace – Now your company is targeted –” (2016)

No.	Title	Topic	Target	Video ID
1	Opening	Cybercrime	Office	CBd9KzGy44o
2	Current situation of cyber crime	Cybercrime	Office	sB8yIse_Gkg
3	Episode 1 for business owner	Cybercrime	Office	6vcP6-Ln0cA
4	Episode 2 for system administrator	Cybercrime	Office	h3Sd4CFsdAY
5	Episode 3 for general employees	Cybercrime	Office	j4F0PeDWNb4
6	Ending	Cybercrime	Office	IgZuvWaIDYk

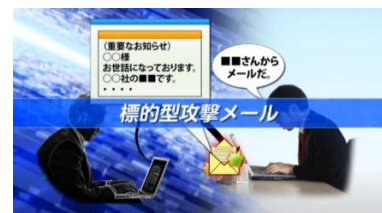


Table-13 Short Video Series Aimed at kids to Learn Risks on the Internet by NPA (2021)

No.	Title	Topic	Target	Video ID
1	What is the internet?	Education	Youth	cSyctN0SfmE
2	Trouble on messaging – OK to send that?	Education	Youth	1Gb7Tafi7SY
3	Spoofing on the net – truth behind the screen	Education	Youth	3ptrQtZv9do
4	Blackmailing of self portraits	Education	Youth	YNo2X8xVnNg
5	Slander on the net – Is that comment OK?	Education	Youth	rmDfS1N1uu8
6	What becomes a cybercrime?	Education	Youth	vRXHiIpeq6c



6.4.3 Safety on the Internet and SNS⁷⁷

Source: Experience based Safety Education Program **Year:** 2019
Target: Parents **Category:** Awareness Raising **Format:** Animation

Rather long (22 minutes) animation for awareness raising for new parents who have preschool children. It raises awareness about dangers of uploading photos of their children on the internet, SNS privacy trouble, etc.



6.4.4 Smartphone & Mobile Phone Family Guide⁷⁸

Source: KDDI **Target:** Family **Category:** Awareness raising **Format:** Animation

Short animation series on the safe usage of smartphones for family, created by a mobile phone operator company. There are 14 episodes in total as follows.

Table-14 Short Animation Series “Smartphone/mobile phone case file” by KDDI

No.	Title	Video ID
1	Too dangerous to watch smartphone while walking	ErSDI_8Pzgo
2	Be careful of smartphone addiction	2lqw1_RluDc
3	Do not bully on the net!	UUOYmJMVA08
4	Uploading photos can be dangerous	T7Wsm4MVXWA
5	Free games are not really free	Bj4067gxmCY
6	Be careful what you write into SNS	0t0Zo011Sg4
7	Photos can tell your home address	TEGh_1f5ixQ
8	Writing bad message will return to you	9lHYo64cZCs
9	Stop illegal download	dSPmWQ_hPYg
10	Do not let your guard down on smartphone apps	rTI5ucPsKt8
11	One click can be fatal	dLB5QtDBM50
12	Turns out to be a bad guy	UeJT43Gzib4
13	Stolen personal information	-m4r926X0aI
14	You will lose your friends by chain mail	TADKOrFdopY



⁷⁷ <http://www.safety-education.org/インターネット・snsの安全/>

⁷⁸ <http://www.kddi.com/family/>

6.4.5 Let's Experience the Dangerous World of the Internet!⁷⁹

Source: Kanagawa Prefectural Government
Target: Young **Category:** Awareness raising **Format:** Simulation

This is a website to experience simulated danger of the internet developed by Kanagawa prefecture.

It covers common cases of pitfalls as follows.

1. Information theft on fortune telling website
2. One-click fraud demanding money
3. Meet-on-the-net/Community sites
4. Online shopping
5. Online games

Each episode is rather long (~10 minutes) to go through the whole process of being victim and its prevention



6.5 Game/E-learning/Simulation

6.5.1 Let's find out what's "suspicious" on the Internet!⁸⁰

Source: Kaspersky x Shizuoka Univ.
Target: Teachers **Category:** Teaching materials **Format:** Card game

This is a teaching material that employs a card game to teach cybersecurity to students. It won an award as consumer education material in 2018. The cards used in the game are like shown below.



Figure-13 Card Design in the Game for Learning Suspicious Things on the Internet

⁷⁹ <https://www.pref.kanagawa.jp/docs/r7b/cnt/f535323/p415459.html>
⁸⁰ <https://kasperskylabs.jp/activity/teachingmaterial/>

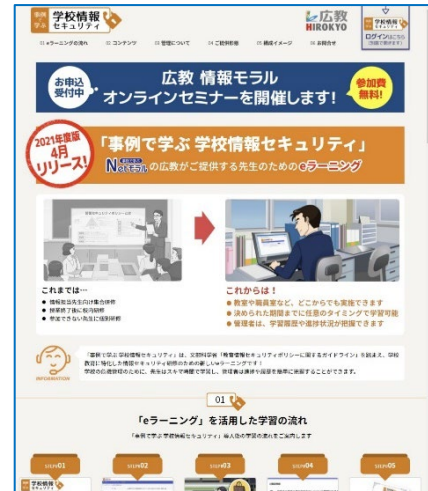
6.5.2 Learning School Information Security through Case Studies⁸¹

Source: Hiroshima Kyohan Co., Ltd.
Target: Office **Category:** Teaching materials **Format:** e-learning

This is a website of a company that develops e-learning materials for cybersecurity in schools by case studies. In this e-learning course, the learner will learn through multiple videos featuring cybersecurity topics encountered at school. Some of the topics covered are:

- Password security
- Phishing fraud
- SNS usage

Module for internet morality is also available⁸².

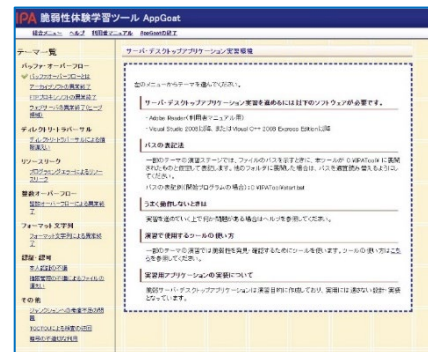


6.5.3 Vulnerability Experience Learning Tool: AppGoat⁸³

Source: IPA **Target:** Developer **Category:** Training **Format:** Simulation

This is a simulation software to experiencing vulnerability of Web application. It is designed for novice programmers who are engaging in Web development. In this software, many common vulnerabilities such as the following are simulated.

- Buffer overflow
- Abnormal termination of archiving software
- Abnormal termination of FTP proxy
- Abnormal termination of Web server
- Directory traversal
- Resource leakage



6.5.4 Cybersecurity Education Game⁸⁴

Source: JNSA **Target:** General **Category:** Active learning **Format:** Game

These games are developed by the “game education” working group of the JNSA education committee. The group is trying to prove the effectiveness of game-based learning for CSIRT role playing.



⁸¹ <https://www.hirokyou.co.jp/iss/>
⁸² <https://www.hirokyou.co.jp/netmoral/e-learning/>
⁸³ <https://www.ipa.go.jp/security/vuln/appgoat/>
⁸⁴ <https://www.jnsa.org/edu/secgame/>

Currently two games are published:

- Security expert “Werewolf” game⁸⁵
- Malware Containment

6.5.5 Phishing fraud VR “Where is the criminal?”⁸⁶

Source: NPA **Target:** General **Category:** Awareness raising **Format:** VR Video

NPA created a phishing scam prevention VR video in 2020. It has a story of an SMS from a criminal disguised as a financial institution leading to a fake site, and the victim is fooled to do fraudulent remittance by breaking two-factor authentication. VR helps as if the viewer becomes the victim in the story.



7. Experiences, Knowledge, and Issues related to Awareness Raising Activities in Japan

7.1 Awareness Survey on Ethics and Threats of Information Security⁸⁷

Source: IPA **Year:** 2020 **Target:** General **Category:** Survey **Format:** PDF

This is the latest survey on the awareness of cybersecurity conducted by IPA. There are two volumes: A report on “Ethics” and a report on “Threats”.

According to this survey result, for example, young people, especially teenagers, have a significantly higher experience of receiving education on information security through elementary and junior high schools than other age groups. But their knowledge of specific threats and awareness of the risks of disclosing personal information are not significantly higher than other age groups, and in some cases are even lower as shown in the figure below.



⁸⁵ <https://www.youtube.com/watch?v=h87srzDLx0>
⁸⁶ <https://www.youtube.com/watch?v=YG4rT9-nxGY>
⁸⁷ <https://www.ipa.go.jp/security/economics/ishikichousa2020.html>

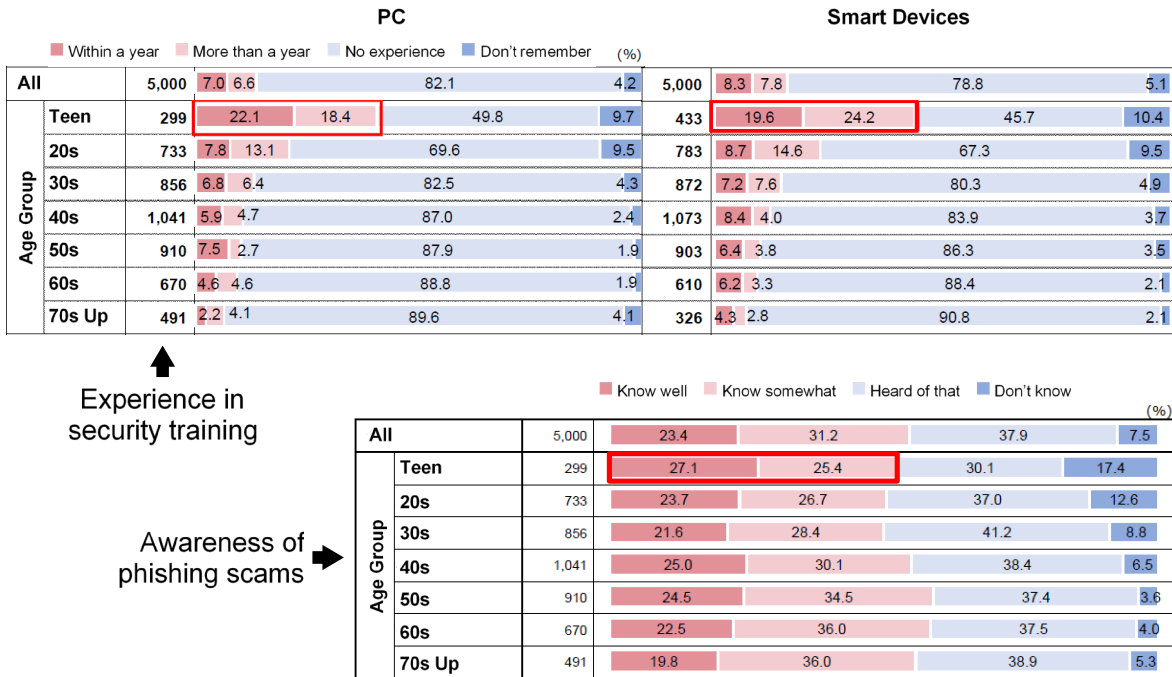


Figure-14 Security Education and Awareness on Phishing Scams by Age Group in Japan

7.2 Survey Report on Security Trends in Corporate Organizations⁸⁸

Source: Trend Micro **Year:** 2020 **Target:** Enterprises **Category:** Survey
Format: PDF

This is the survey report on cybersecurity situation in organizations and enterprises of Japan. The survey was conducted in June 2020, targeting risk management, IT systems, and information security personnel at public agencies, local governments, and private companies in Japan, to identify the occurrence of security incidents, the effectiveness of management security leadership, and concerns about IT environments and systems. Notable trends found in the survey result are as follows.

- Ransomware attacks are growing.
- Security concern is rising on teleworking.
- Higher amount of damage caused by security incidents as shown in the figure below.



⁸⁸ https://www.trendmicro.com/ja_jp/about/press-release/2020/pr-20201002-01.html

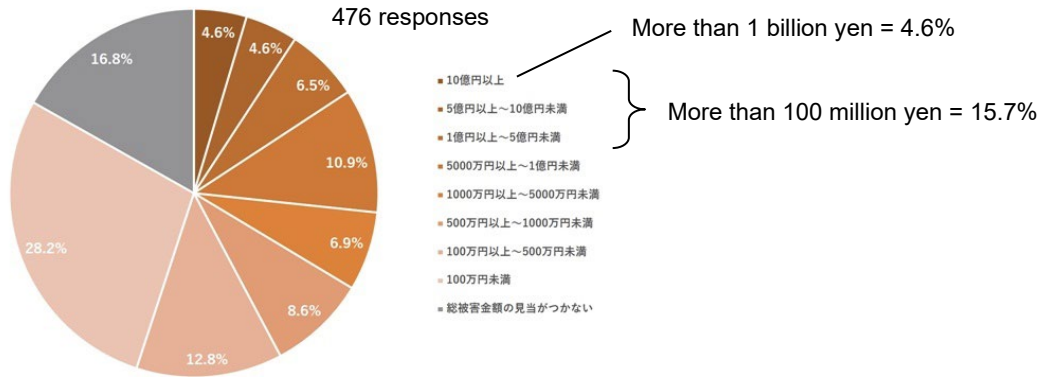


Figure-15 Damage Amount of Security Incidents in Japan

7.3 Whitepaper on Crime (Ministry of Justice)⁸⁹

Source: MOJ **Year:** 2020 **Target:** General **Category:** White paper
Format: PDF

This is a part of the annual whitepaper issued by the Ministry of Justice of Japan regarding the current situation and trends of crimes in Japan. This part (Part 4) is dedicated to the detailed trend analysis of each crime type and its judgment. Chapter 4 is about cybercrime and Chapter 5 is about domestic violence, child negligence, and stalkers. According to this whitepaper, the trends of cybercrime in Japan are as follows.

- Number of cybercrimes is increasing as shown in the figure below.
- Of all cybercrimes in 2019, 40% were child-related

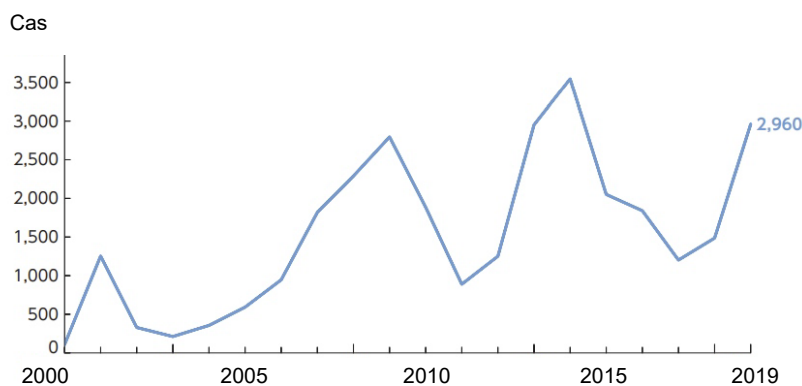
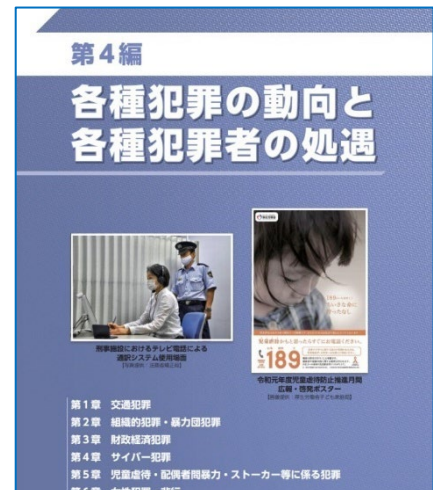


Figure-16 Increasing cybercrime cases in Japan (Whitepaper on crime)

⁸⁹ <https://www.moj.go.jp/content/001338447.pdf>

8. Characteristics of Awareness Raising Activities for each Target Audience in Japan

8.1 Overall Characteristics of Awareness Raising Materials in Japan

- (1) Manga (Cartoon) and animation are extremely common
 - Japanese are traditionally good at “grasping” the whole picture/concept by sight (pictures).
 - The popularity of these sight-based media is not only for kids, but also for adults.
 - Even serious contents often employ cartoon-like characters.
- (2) Real videos/photos sometimes contain too much noise
 - Simplified representation of Manga/Animation can focus on the important points
- (3) Content that “forces” or “dictates” the message often fails in Japan
 - Intimacy/friendliness is more important than authority/power
 - Some comedy tastes will give better experience to the audience



Figure-17 Manga Comedy to Promote Strong Password by IPA

8.2 Issues on Child Protection in Japan

There are the following issues on child protection in Japan.

- Bullying is serious problem in Japan⁹⁰.
 - The same tendency on the net. Anonymous attacking to others via SNS are very common.
 - Bullying of kid players in online games by elder players are also common
- Meet-on-the-net (online matching) cases are also growing in Japan
 - Serious problem among secondary to high school students
 - Often leading to blackmailing threats to sexual attacks

⁹⁰ <https://savvytokyo.com/bullying-japanese-schools/>

- Therefore, there are many awareness raising materials for preventing children from being caught in those cases
 - But a real problem is that the target generation is not interested in awareness raising materials
 - Need to approach them through something that “they are interested in” such as pop music or influencers on the net (such as YouTubers).

8.3 Cybersecurity of elderly people in Japan

There are the following characteristics of cybersecurity for elderly people in Japan.

- Elderly people in Japan are always the target of “Ore” fraud⁹¹.
 - Scammers pretending to be relatives (typically a son) try to steal money from elderly people through telephone.
 - Now more elderly people are starting to use smartphones, and all sorts of phishing attack are added to the traditional telephone-based fraud.
- Elderly people are as vulnerable to frauds as children
 - But they have more money, and they are reluctant to be controlled by filtering tools
 - Thus, they are more vulnerable to cyber-fraud attacks
- Countermeasures for these frauds include:
 - Specifically designed smartphone for elderly people that has limited and safe functionality
 - Awareness raising activities/materials for the older generation are emerging



Figure-18 Example of Smartphone Designed for Elderly People

9. Strategies and Theories for Awareness Raising Activities in Japan

9.1.1 New Information Security Promotion and Awareness Program⁹²

Source: Information Security Policy Council **Year:** 2014

This is three years program issued by the government for promoting people’s awareness on the cybersecurity. The program contains the following activities, and some of them are still being implemented after three years.

⁹¹ <https://www.transenzjapan.com/blog/scams-and-the-international-family/>

⁹² <https://www.nisc.go.jp/active/kihon/pdf/awareness2014.pdf>

(1) Promotion of comprehensive and intensive dissemination and awareness raising measures

- Setup related national day and month:
 - “National Cybersecurity Day” (2nd Feb.)
 - “National Cybersecurity Training Day” (18th Mar.)
 - “Cybersecurity Awareness Month” (2/1-3/18)⁹³

These are setup in February-March because the awareness should be raised during the end of fiscal year in Japan when many organizations in Japan are very busy.

(2) Regional promotional events (prefecture level)

In each region of Japan, there are examples of local initiatives (councils of related organizations and groups) that utilize their specific expertise and ingenuity. For example, private companies for filtering and e-mail settings, the local police for information on crimes and damage caused by internet use, and PTAs and parents’ groups as instructors for making rules at home. In this way, there are examples of the formation of local bodies (councils of related organizations and groups) while utilizing the expertise and creativity of each organization. Such efforts to promote cooperation among related parties in the region, mainly by sharing case studies, creating teaching materials, and dispatching lecturers, as well as widely utilizing the created teaching materials, will contribute to the revitalization of activities in each region, and are considered to be extremely effective from the perspective of approaching each citizen.

In addition, those who are interested in information security in the region and have the awareness to communicate the information to others should be certified as the information security supporters to promote promotion and enlightenment in the region through actions to support their activities to promote safe and secure IT utilization.

(3) Specific actions for each target group:

- General public as a whole
 - Setup websites related to cybersecurity
 - Promote the logo for Cybersecurity Awareness Raising
 - Utilize media (comics, songs, etc.) and collaboration with creators.
 - Implement seminars, training
 - Fostering volunteers for awareness raising



Figure-19 Logo for Cybersecurity Awareness Raising
(Know - Protect - Continue)

⁹³ <https://www.nisc.go.jp/security-site/month/index.html>

- Elementary and secondary education
 - Establishing information literacy
 - Promotion of information moral education
 - Awareness raising of parents
 - Development of educational contents and their dissemination
 - Appropriate and safe usage of IT related equipment and services such as smartphones and SNS
 - Competitions for slogans and posters related to cybersecurity
- Those who have less opportunity to learn cybersecurity
 - Easy-to-understand awareness raising contents for Housewives, Aged people, etc.
 - Expanding consultation service and preparation of FAQ
- Those who are not interested in cybersecurity
 - Provide specific measures to promote cybersecurity such as sending email cautionaries and notifications from school to parents.
- Business managers and employees
 - Seminars for training cybersecurity leaders in SMEs, awareness raising seminars for managers
 - Awareness raising activities and events through regional chamber of commerce and industry associations, and provision of cybersecurity rescue support such as J-CRAT (→2.2.3)
 - Provides awareness raising materials (leaflets, e-learning, etc.) for employees
- Strengthen international collaboration
 - Information security international campaign⁹⁴
 - ASEAN-Japan Cybersecurity Policy Meeting⁹⁵

9.1.2 Cybersecurity Awareness and Action Enhancement Program⁹⁶

Source: Cybersecurity Strategy Headquarters **Year:** 2019

This summarizes awareness raising programs under implementation in both public and private sectors that are revised annually based on the updated cybersecurity situation in the world (see Chapter 5 for details). There are four fundamental directions for the promotion of awareness raising presented in this program:

⁹⁴ https://www.nisc.go.jp/conference/seisaku/jinzai_wg/dai12/pdf/shiryoku2.pdf

⁹⁵ https://www.meti.go.jp/english/press/2021/1022_001.html

⁹⁶ <https://www.nisc.go.jp/active/kihon/pdf/awareness2019.pdf>

- (1) Promote “awareness and action” in individuals and organizations
- (2) Promote awareness from “three viewpoints”
 1. Continuous implementation
 2. Provision of appropriate tools and contents for each target
 3. Promotion of collaboration among related parties

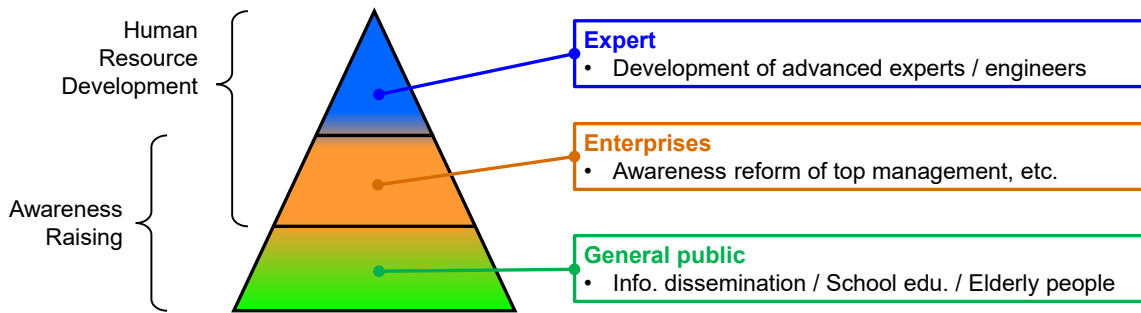


Figure-20 Overview of the Cybersecurity Awareness Raising Program

10. Marketing Methods and Theories for Awareness Raising Activities

10.1 Why Marketing?

10.1.1 Why Marketing for Cybersecurity Awareness Raising Activities?

- Possible issue 1: Your target audience is likely to miss (not recognize) your content.
- Possible issue 2: Your target audience is not likely to take action, even if you reach them.

There are several typical reasons for awareness raising activity failures. Examples of typical reasons are:

- (1) Not clarifying your target.
 - No consensus among an organization.
- (2) Not understanding your target audience path.
- (3) Your target audience and channels are not matched.
- (4) “Why important and necessary for the target audience” is not clearly stated.

10.1.2 Examples of Solution (Marketing Approach)

For example, the prementioned issues are solved with several marketing approaches as below.

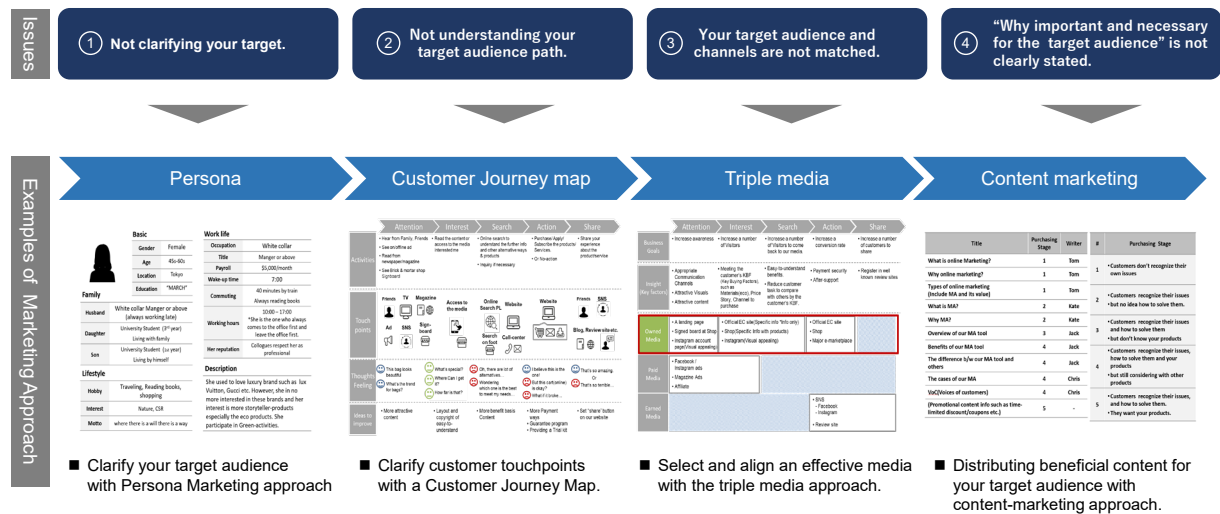


Figure-21 Examples of Marketing Approaches

10.2 What is Marketing?

10.2.1 Definition of Marketing

Simply put, marketing is meeting needs profitably without selling. The following are popular examples of definitions of marketing.

- (1) American Marketing Association⁹⁷

“Marketing is the activity, set of institutions, and processes for creating, communicating, delivering, and exchanging offerings that have value for customers, clients, partners, and society at large.” (Approved July 2013)

- (2) Peter Drucker⁹⁸ (Austrian-American management consultant, educator, and author)

“The aim of marketing is to make selling superfluous.”

- (3) Philip Kotler⁹⁹ (American marketing author, consultant, and professor)

“meeting needs profitably.”

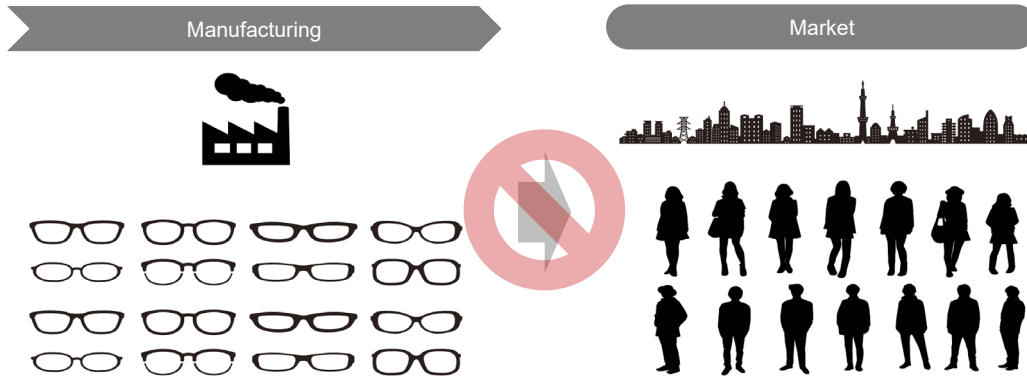
⁹⁷ <https://www.ama.org/>

⁹⁸ https://en.wikipedia.org/wiki/Peter_Drucker

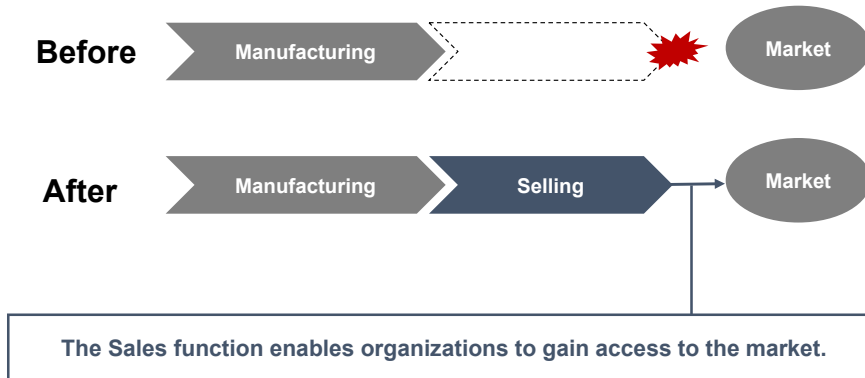
⁹⁹ https://en.wikipedia.org/wiki/Philip_Kotler

10.2.2 What if there is no Marketing/Selling?

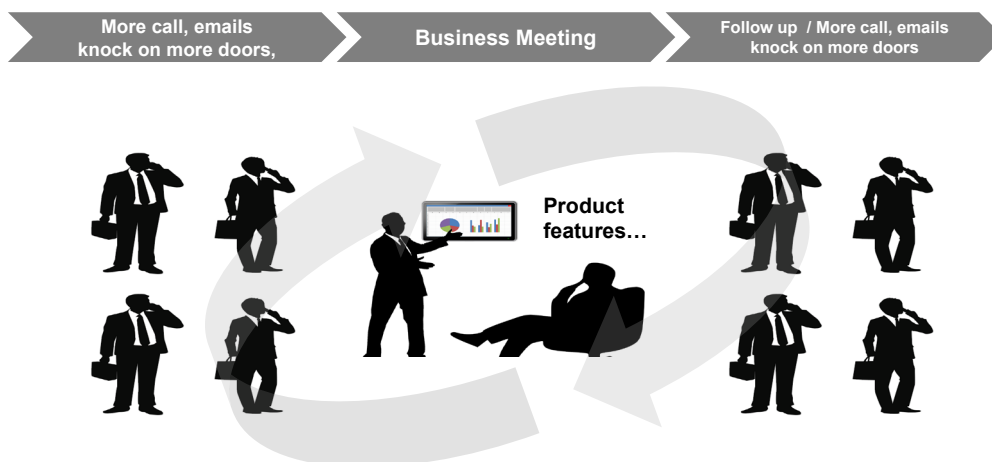
If you just make products (manufacturing) and do no marketing, then your products/services hardly sell because no one *recognizes* them.



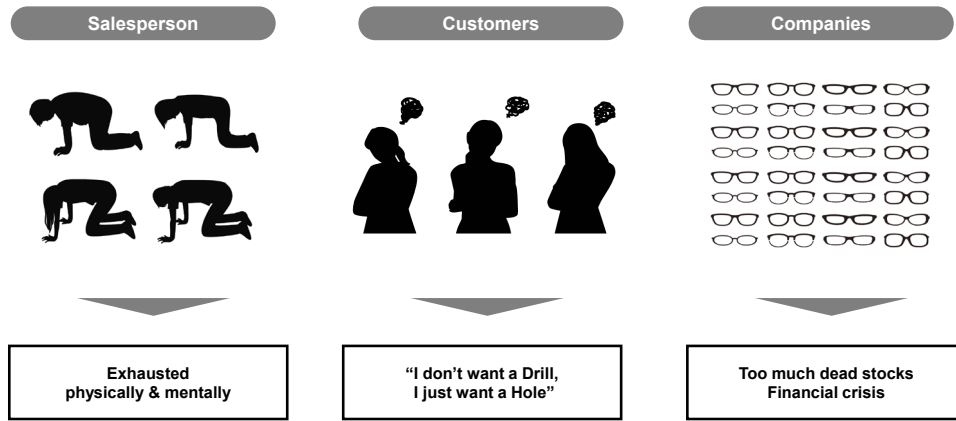
Then, a sales function is required for the companies/organizations.



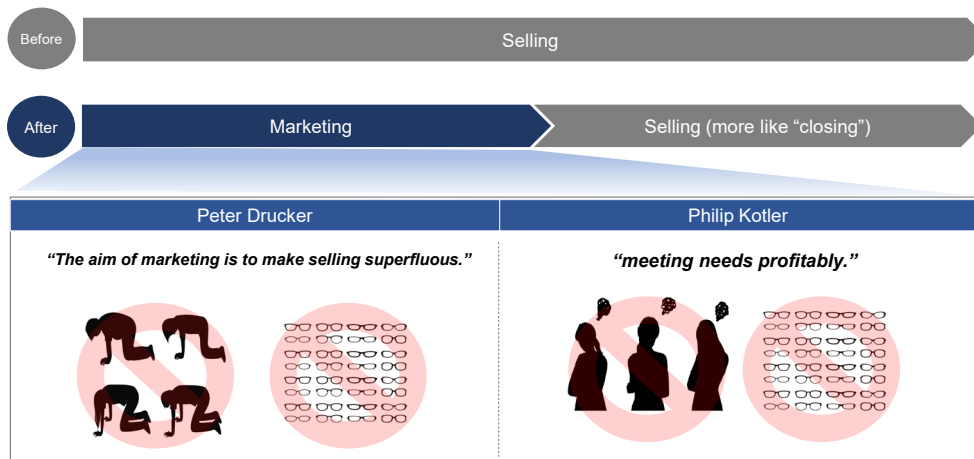
However, the conventional selling approach is more like “push-selling” and “product-out”



For example, the digital camera market in Japan once pursued resolution competition without considering the views of customers. Once the number of pixels exceeds a certain number, it no longer becomes Key Buying Factor for customers. But companies kept pursuing higher numbers of pixels because they didn't consider views of customers. As a result, no one is happy if you continue push-selling.



Thus, a marketing function is significantly required for companies/organizations to be “going concerns”.



10.3 Overview of Marketing Process

Simply, Not Product-out but Market-in approach is required like shown in the figure below.



10.3.1 Market Research



(1) Objective of Market Research

The objective of market research for businesses is to identify market opportunities for companies/organizations.

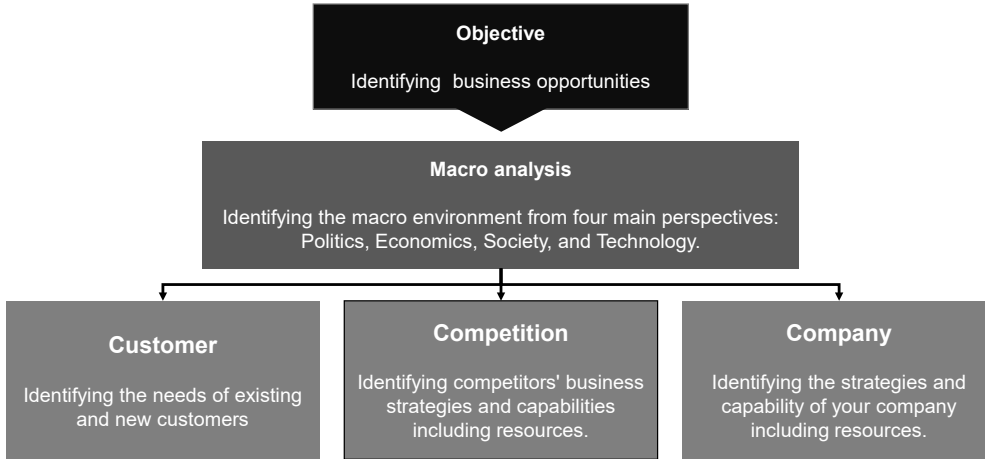
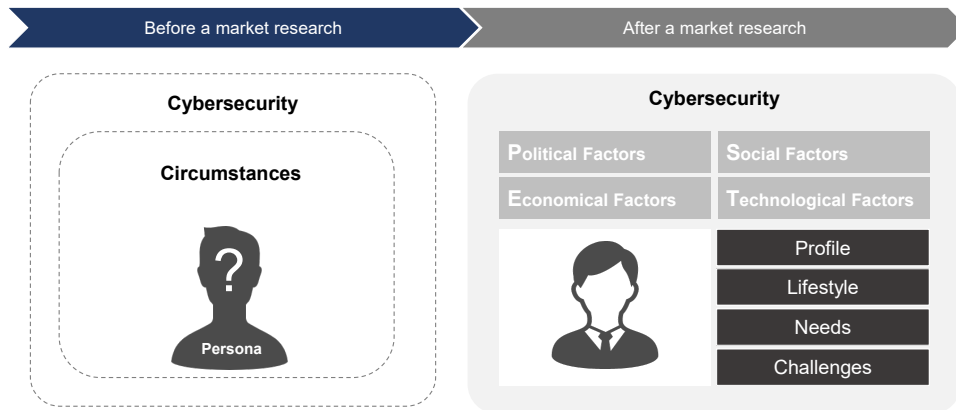


Figure-22 Objective of Market Research for Business

For cybersecurity awareness raising activities, market research means identifying the status of cybersecurity in Vietnam in aspect of cybersecurity awareness raising.

For example, their circumstances/environment, who's been suffering, their challenges/problems, etc.



(2) Major frameworks for market research

There are several frameworks available such as PEST, 3C, SWOT Analysis etc. Which framework will fit to your project depends on your objectives, organization types, etc.

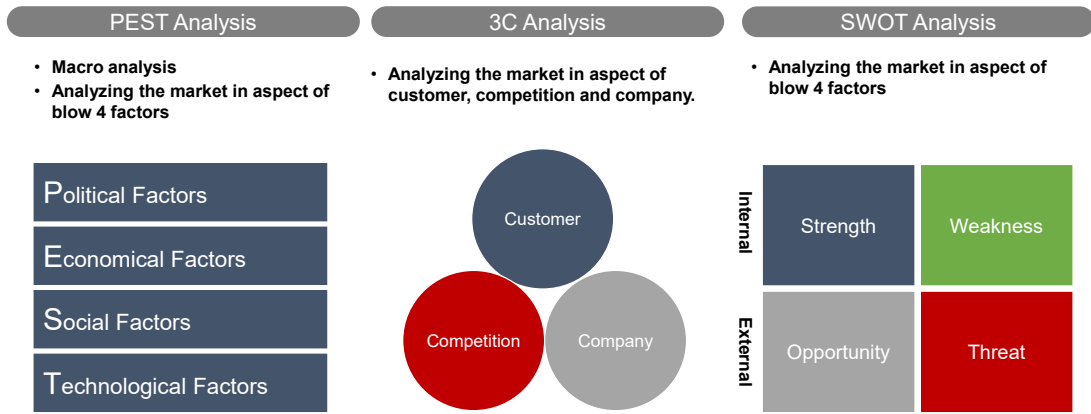
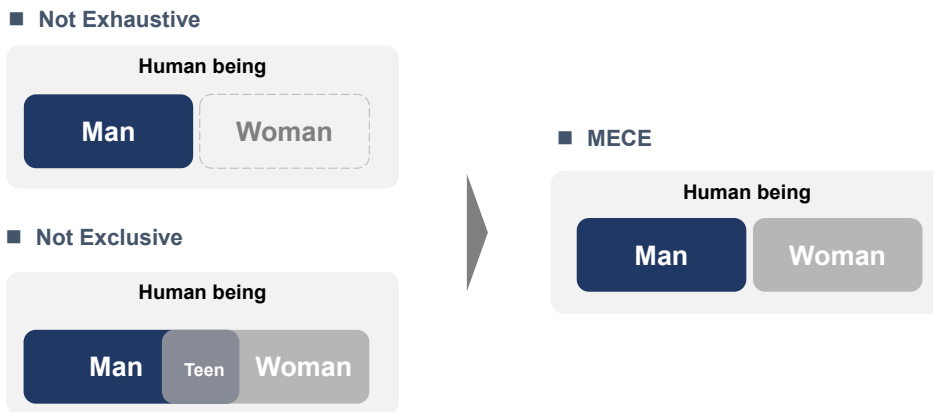


Figure-23 Examples of Market Research Framework

(3) Tips for market research

Tips 1: MECE (Mutually Exclusive, Collectively Exhaustive)

MECE-mind makes your research more accurate.



Tips 2: Types of Data

Gaining first party data is important option when data is not available.

Table-15 Types of Data for Market Research

Type of data	Explanation
1st-party Data	Your own data (Primary research)
2nd-party Data	First data researched by governments, public organizations, other companies etc.
3rd-party Data	Data based on several external sources.

Note: It doesn't mean 3rd party data is less important. It depends on the purposes.

Tips 3: Hypothesis

It is important to have a hypothesis before researching from the aspect of efficiency.

No hypothesis	Testing a hypothesis
<ul style="list-style-type: none"> ■ Taking so much time <ul style="list-style-type: none"> ➢ Keep searching for a longer time due to a lack of clarified criteria to stop. ■ Gaining poorer info/facts <ul style="list-style-type: none"> ➢ Please imagine having an interview with key persons about your topic. Most of your questions is open-questions. You are likely to receive abstract info/facts relatively(compared to the ones who have a hypothesis beforehand.) 	<ul style="list-style-type: none"> ■ Prompt <ul style="list-style-type: none"> ➢ Info you need is ones related to your hypothesis. *You are likely to encounter other key factors during a market research to test your hypothesis. ■ Gaining richer info/facts <ul style="list-style-type: none"> ➢ Please imagine having an interview with key persons about your topic. You are likely to give not only open-questions but also closed-questions because you have a hypothesis(more specific info). You are likely to receive specific info/facts relatively(compared to the ones who don't have a hypothesis beforehand.)

10.3.2 STP Analysis



STP analysis stands for Segmentation, Targeting, and Positioning analyses. It is intended to segment the market, define target segments, and determine your position as shown in the figure below.

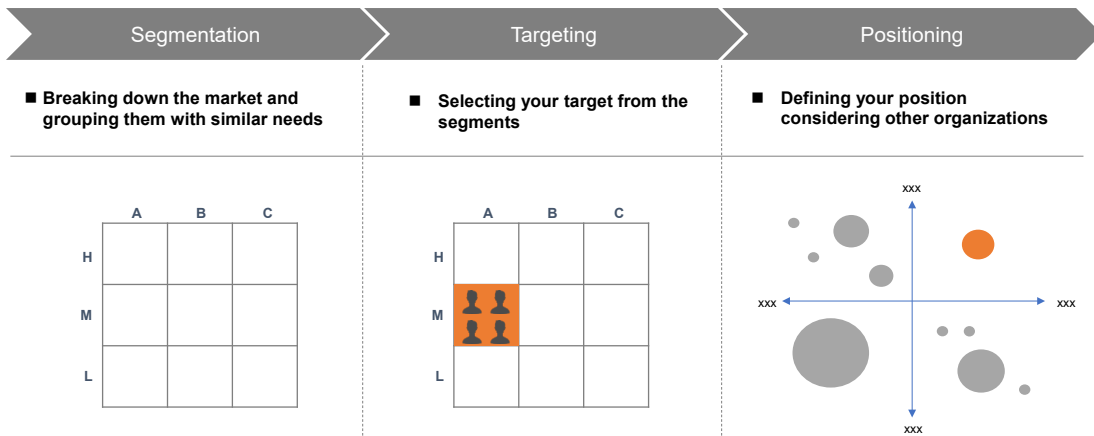
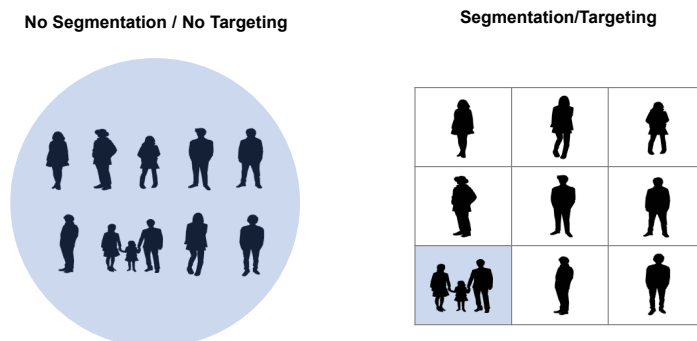


Figure-24 Overview of STP Analysis

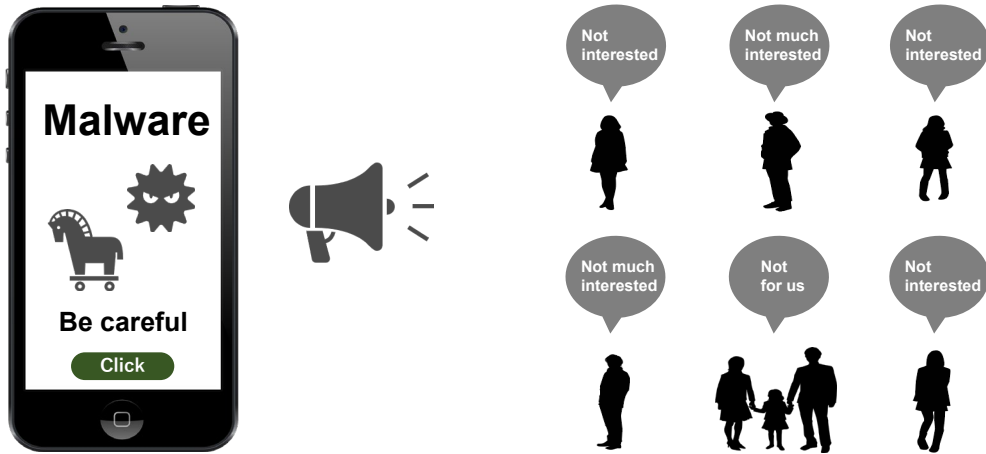
■ Why Segmentation & Targeting?

Because you need to identify suitable audiences for you to be able to reach them with right content.



■ **What if there is No Segmentation/Targeting...?**

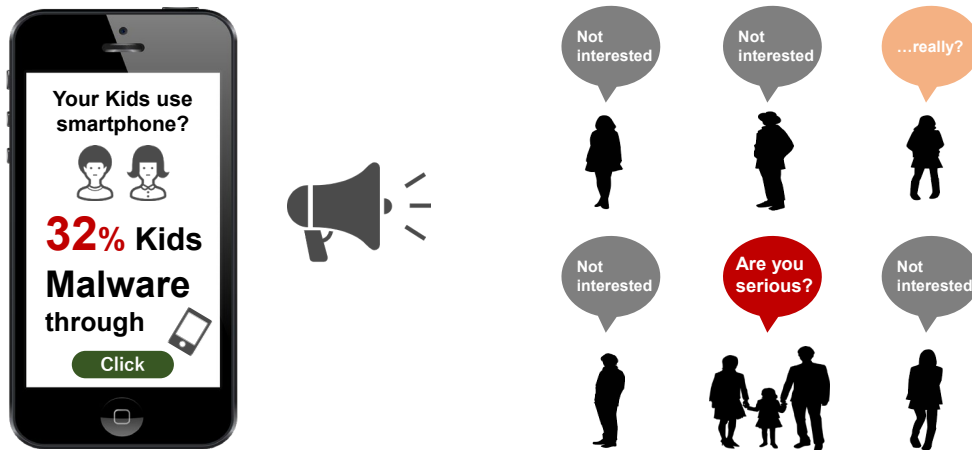
First, it will be very hard to reach your audience. Second, they are not likely to take an action you expect them to do.



It's because your strategy and execution (such as content, channels, etc.) are not aligned with your target audience's behavior.

■ **Benefit of appropriate Segmentation/Targeting**

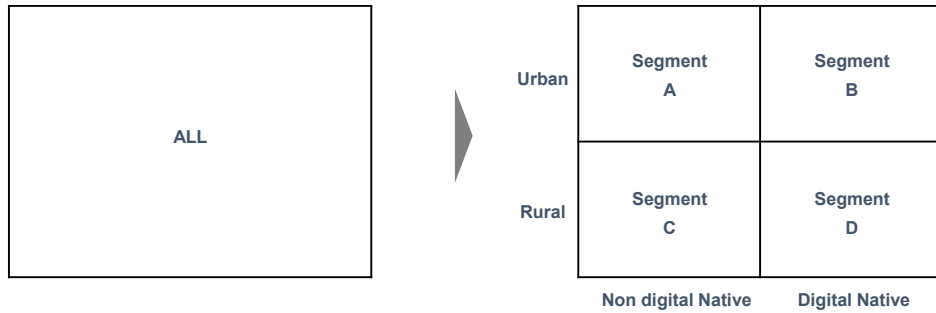
Your target audience is likely to react in the way you expect them to do.



Your strategy and execution are aligned with your target audiences.

(1) Segmentation process

Segmentation process is intended to break down the market and group them with similar needs.



*It doesn't have to be four quadrants. It depends on your project.

Targeting without segmentation makes the target customers unclear. As a result, both strategy and operations, including external messages, will be inconsistent.

Several factors are used for segmentation such as the following.

① Demographic factors

Gender, Age, Occupation, Income, Family size, Religion, Language, Culture etc.

② Geographical factors

Country/Area, Population, Economy, Weather etc.

③ Psychographic factors

Lifestyle, Values, Interests, Personalities, Attitudes, etc.

④ Behavioral factors

Channel, Frequency, Occasion, Usage rate etc.

⑤ Firmographic factors (for B2B)

Industry, Location, Revenue, Number of employees, etc.

There are also several frameworks such as 4R and 6R for criteria that are useful to evaluate the segments.

4R

Criteria	Question
■ Rank	Ranking each of segment by priority?
■ Realistic	Enough market size to make sales and profits?
■ Response	Enable to measure and analyze the response?
■ Reach	Enable to reach the segment effectively?

6R

Criteria
Realistic Scale
Rank
Reach
Response
Rate of Growth
Rival

(2) Targeting process

Targeting process is to select your target from the segments.

Example of selecting target segment:

Criteria	Segment A	Segment B	Segment C	Segment D
① Enough market size	1st	3rd	2nd	1st
② Higher Potential Growth	3rd	3rd	1st	3rd
③ Fit to your organization *You are the most appropriate one considering your role in the field.	2nd	3rd	1st	3rd
④ Enable to measure and analyze the response?	3rd	2nd	1st	2nd
⑤ Enable to reach the segment	1st	3rd	2nd	3rd
⑥ _____	3rd	2nd	1st	2nd
	○	✗	◎	▲

(3) Positioning

Positioning is more like “Differentiation” based on customer needs & competitor approaches.

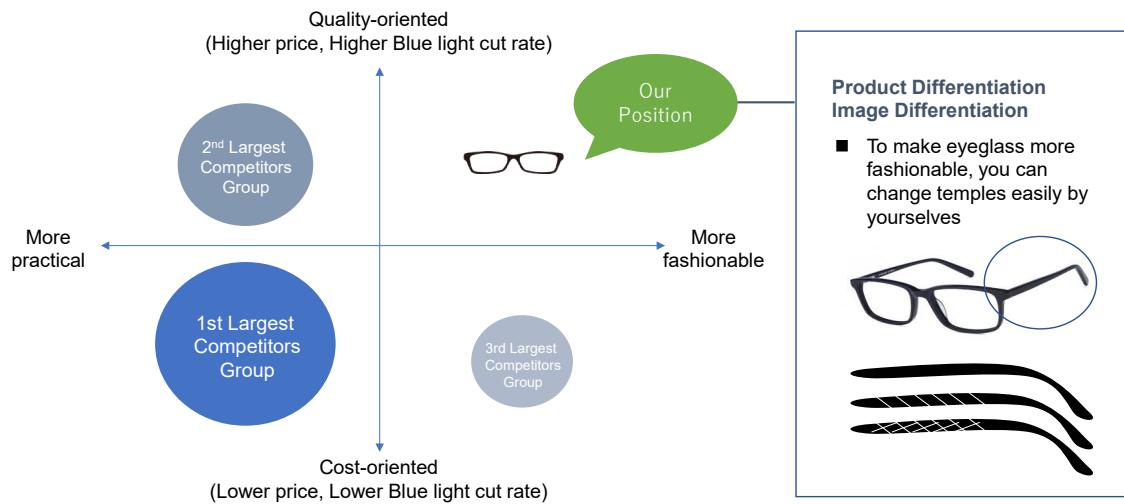


Figure-25 Example of Conventional Cases for Product/Service Positioning (PC Eyeglass)

Criteria for Positioning:

You need to clarify requirements to achieve your positioning strategy.

Rough estimate sheet for requirement, Feasibility and Cost

Requirement	Feasibility	Cost
① Changeable temple mechanism	Possible (Inhouse)	Possible (\$30,000)
② Sophisticated temple Design	Possible (Inhouse)	Possible (\$10,000)
③ Higher Blue light cut lens	Possible (Supplier A)	Possible (\$10/pc)
④ Promotion for branding	Possible (Agency B)	Possible (\$10/pc)

Conclusion
Feasible to achieve the differentiation

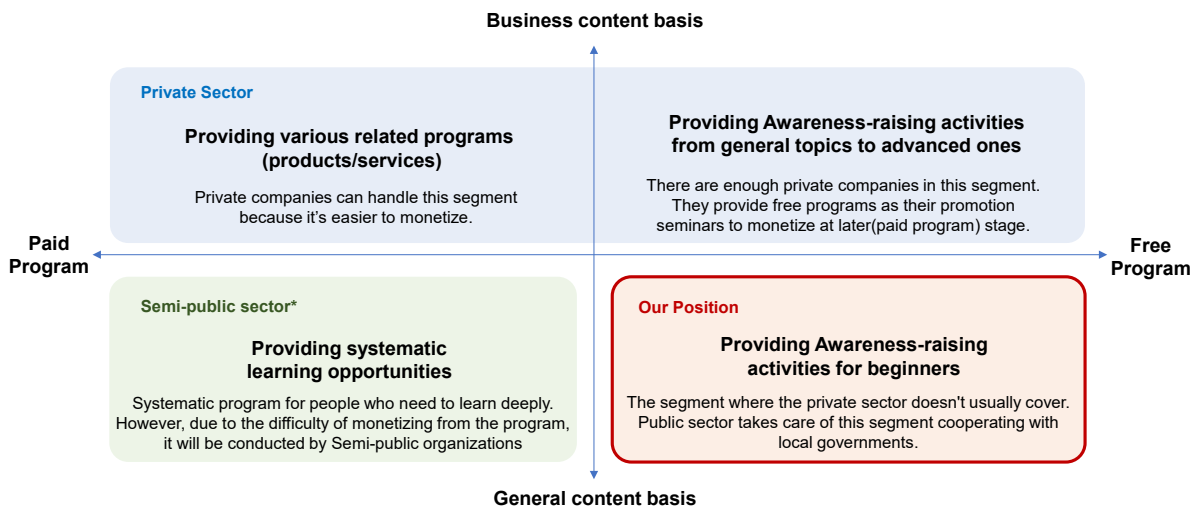
Reference - Differentiation:

Major factors for differentiation are as below.

- ① **Product Differentiation**
(More like Functions/Spec)
- ② **Service Differentiation**
(Customer Service, Delivery, expertise, Hospitality etc.)
- ③ **Channel Differentiation**
(Coverage, Easy to access etc.)
- ④ **Price Differentiation**
(Lower price, Dynamic pricing etc.)
- ⑤ **Image Differentiation**
(More like Branding)

Example of positioning map:

Defining your position based on your roles considering other organizations' roles and characteristics.



*Semi-public sector: Business venture financed jointly by the public and private sectors

Figure-26 Example of Positioning Map for Cybersecurity Awareness Raising Activity

Worksheets for performing STP analysis are provided in Appendix 1.

10.3.3 Marketing Mix



(1) What is Marketing Mix?

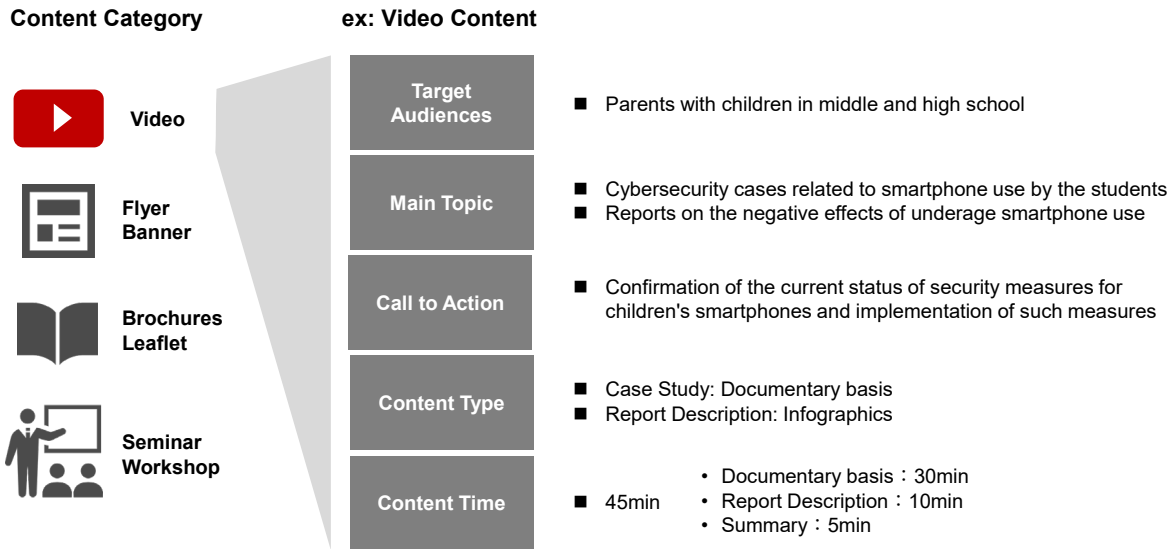
It is specifying your strategy to reach your right audience with right time, channels and content. Normally you will mix one of manufacturing/supplier perspectives (Product/Price/Place/Promotion) with one of customer/user perspectives (Customer value/Cost/Convenience/Communication) like shown in the figure below.



Figure-27 Standard Framework of Marketing Mix

(2) Product/Customer Value

Describe your content in detail. An example for cybersecurity awareness raising activity is as follows.



(3) Price/Cost

There are three major pricing methods.

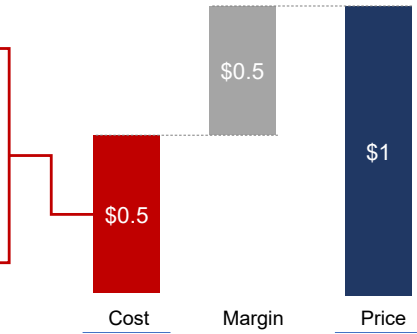
Cost-based Pricing:

Setting price by adding margin on the cost.

Ex. Bottle of water



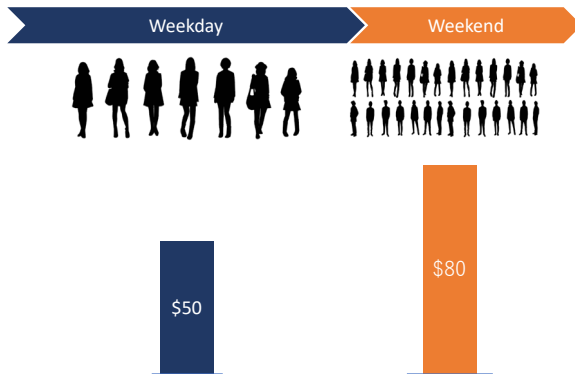
Cost for 500ml natural water
 - COGS(Cost of goods sold): 35 cents
 Water: 15 cents
 Bottle, Cap and others: 20 cents
 - SGA: 25 cents
 (sales, general, and administrative expenses)



Demand-based Pricing:

Setting price depending on volume of user demand.

Ex. Hotel pricing



Ex. Industry

- Hotel
- Airlines
- Entertainment (Ticket etc.)

Competition-based Pricing:

Setting price depending on competitors' prices.

Ex. Pens

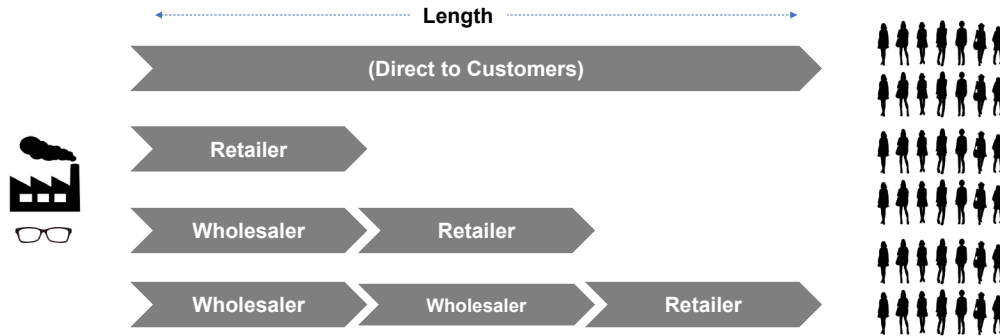


Company A	\$1.1
Company B	\$1.0
Company C	\$0.9
Our company	\$1.0

(4) Place/Convenience

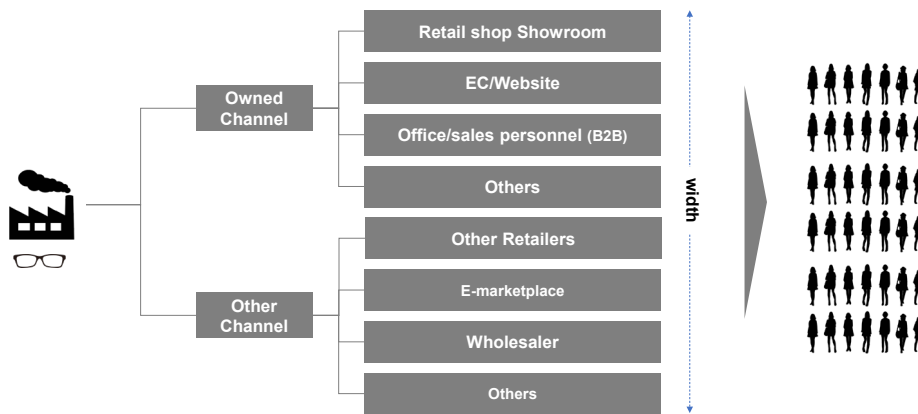
When developing channel strategy, its length is important.

Case: BtoC product channel



When developing channel strategy, its width is important.


Examples of channel




There are intensive, selective and exclusive distributing ways.

Examples of channel


- ① **Intensive Distribution**


 - Providing saturation coverage of the market by using all available outlets

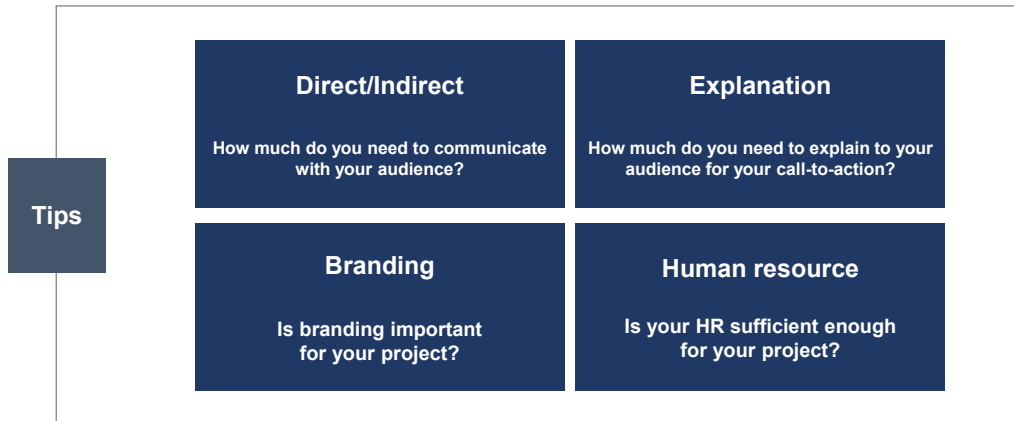
- ② **Selective Distribution**


 - Choosing partners with certain factors and Limiting number of outlets

- ③ **Exclusive Distribution**


 - Providing an exclusive right under certain conditions

The following four viewpoints help you develop channel strategy.



(5) Promotion/Communication

It's important to mix several promotional approaches.



Figure-28 Promotional Mix

It's important to approach each phase of the customer path.

Examples of theory for Customer path

AIDMA by Samuel Roland Hall



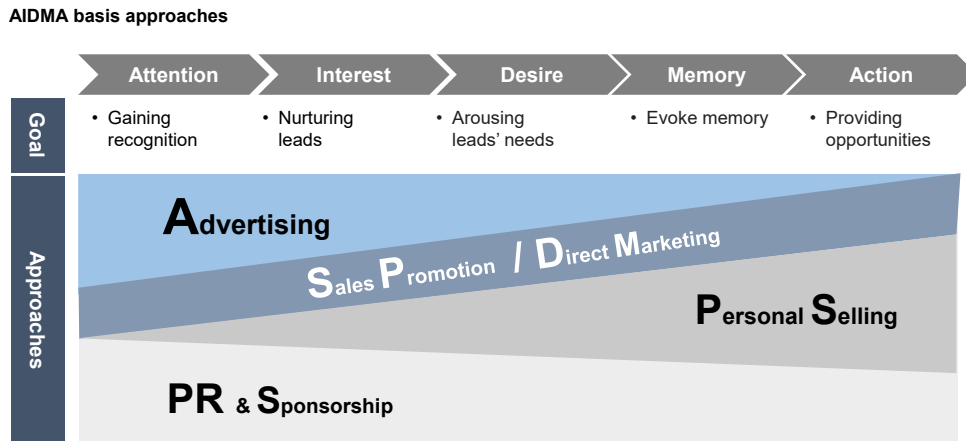
AISAS by Dentsu



5A by Philip Kotler



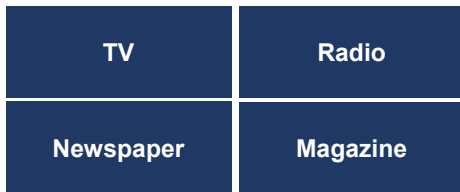
It's important to approach each phase of the customer path.



Source: Modified contents on globis website, “MBA marketing”

Online services are quantitatively measurable and relatively cheaper.

Conventional promotion



COST: Higher
PDCA: Difficult to measure the performance

Online promotion



COST: lower
PDCA: Easier because online media is trackable.

10.3.4 KGI/KPI Setting



Setting KGI (Key Goal Indicator) and KPI (Key Performance Indicator) is necessary for measuring the effectiveness of awareness raising activities, and they can be used for PDCA cycle of improvements for the activities.

KGI must be a measurable value (metrics) that indicates how much your important goal has been reached. It is therefore measurable only when your activity has been (at least partially) performed and all necessary metrics are obtained. In that sense, KGI is a lagging indicator that you will get after some activities are done. On the other hand, KPI is a leading indicator, which points out how well an activity is currently executing towards its goal of achieving KGI. Often, they are used to measure values such as benefits, efficiency, effectiveness, quality and satisfaction. The relation of KGI and KPI is illustrated in the figure below.

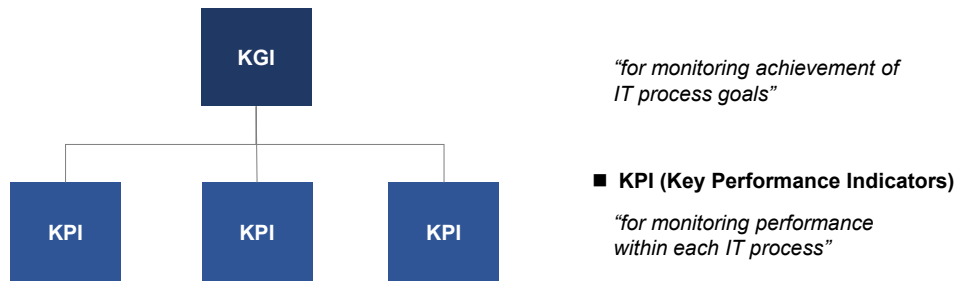


Figure-29 Relation of KGI and KPI

As an example of KGI/KPI for cybersecurity, JCIC (Japan Cybersecurity Innovation Committee)¹⁰⁰ has defined the cybersecurity KPI model for business depending on the maturity of organization as follows.

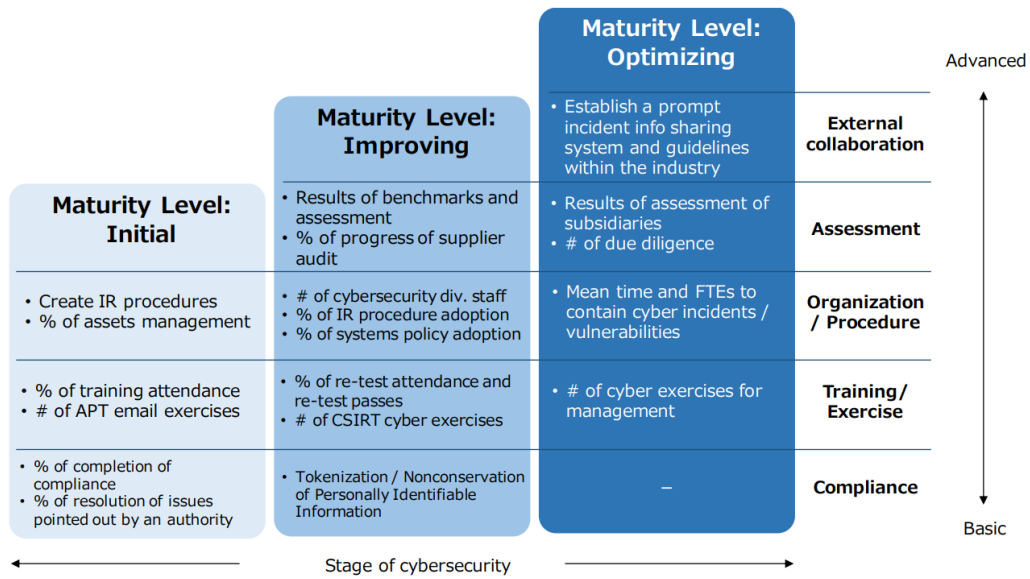


Figure-30 Maturity Stage of Cybersecurity defined by JCIC

JCIC then established example KPIs for cybersecurity readiness as shown in the table below.

Table-16 Example of JCIC’s KPI for Cybersecurity Readiness

KPI	Rough target figures
Compliance rate with laws, regulations, and guidelines	100%
Completion rate for issues raised by regulatory agencies	100%
Number of employees in security department	Over 5% of IT staffs Over 0.25% of TTL staffs
Number of employees who have cybersecurity qualification	Set up based on company’s status
Ratio of cybersecurity budget to total IT budget	Over 7%
Cybersecurity budget consumption ratio	Over 95%
Assessment result	Set up based on company’s status
Number of cybersecurity trainings conducted	Set up based on company’s status
Average time to discover an incident	
Average time and HR to solve an incident	
Average time to discover a vulnerability	
Average time and HR to solve a vulnerability	
Building an information sharing system within the industry	
Security training participation rate	over 95%
Test passing rate of security training	over 85%
Establishing procedures for responding to accidents	No delay against your plan

¹⁰⁰ <https://www.j-cic.com/>

Based on these examples, following is an example of KGI/KPI in an annual plan for cybersecurity awareness raising activity in Vietnam. In this example, we setup KPI per stage of target audience-path (Awareness – Understanding – Future action).

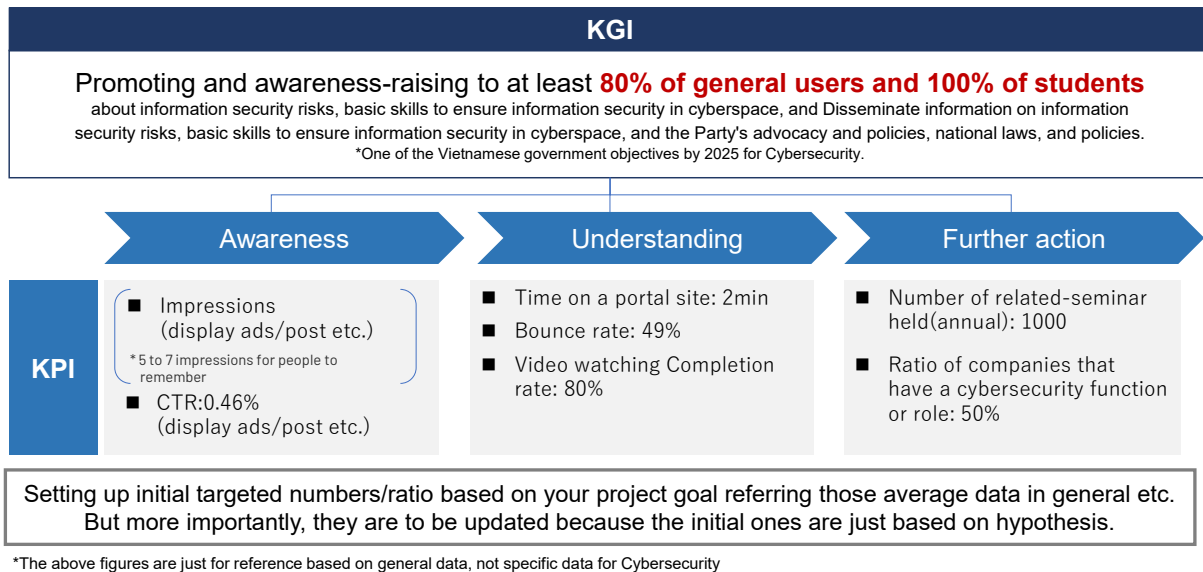


Figure-31 Example KGI/KPI for Awareness Raising activity in Vietnam

When you need to setup KGI/KPI by yourself, so called “SMART” framework shown below would help you to setup effective KGI and KPI.

Specific	Being clear, not vague
Measurable	Not like “Increase Sales”
Achievable	Don't set too high goals for KPI and KGI
Relevant	Don't set KPI that has nothing to do with its KGI
Time phased	“No deadline” means nothing.

Figure-32 SMART Framework for Effective KGI/KPI Setting

10.4 Digital Marketing

10.4.1 What is Digital Marketing?

It is a form of direct marketing that links consumers with sellers electronically.

*“Digital marketing is a form of **direct marketing which links consumers with sellers electronically using interactive technologies** like emails, websites, online forums and newsgroups, interactive television, mobile communications etcetera”*

Kotler and Armstrong

Alternative definition: Marketing using digitals (device, tech, media data etc.).

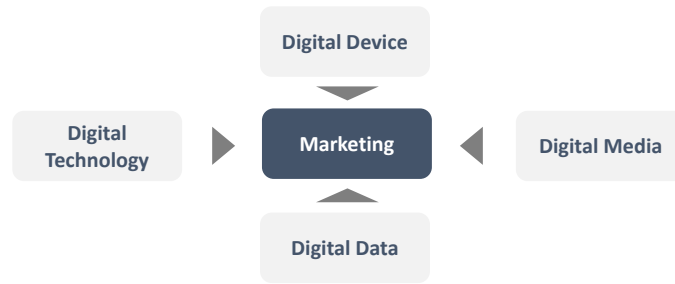
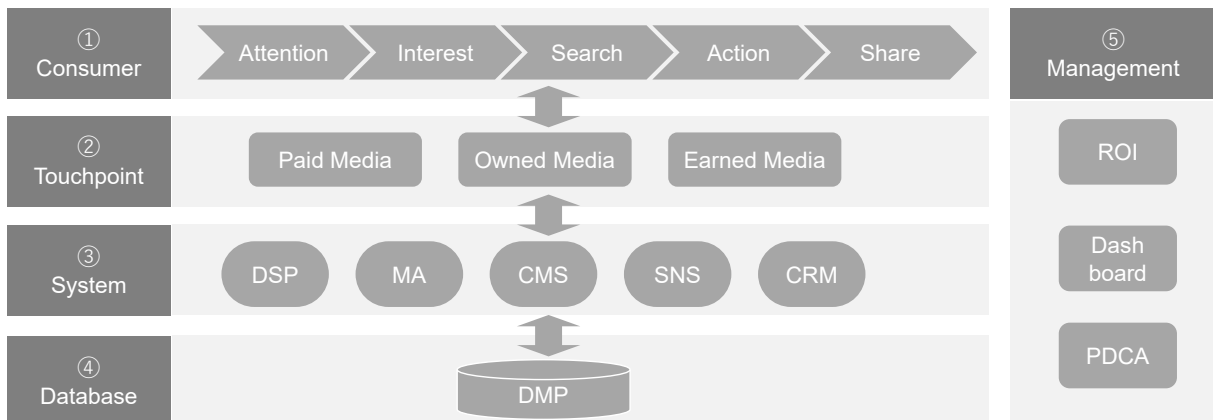


Figure-33 Definition of Digital Marketing by Dentsu

Important Caution: Digital Marketing is not a replacement of Traditional Marketing. Both of Traditional Marketing and Digital Marketing are required.

Overview of Digital Marketing

Digital marketing consists of five factors as shown in the figure below.



Source: Modified Digital Marketing; 10 theories to lead success (Dentsu Digital)

Figure-34 Overview of Digital Marketing

What is the point of marketing in the digital era?

Marketing strategy needs to be corresponded to the three changes in the digital era.



Figure-35 The Three Changes due to Digitalization

10.4.2 Change of Customer Behavior in Digital Era

(1) The way to find Info 4/4

Both of Consumers(B2C) and B2B Buyers search content online for decision making.

AIDMA by Samuel Roland Hall



AISAS by Dentsu



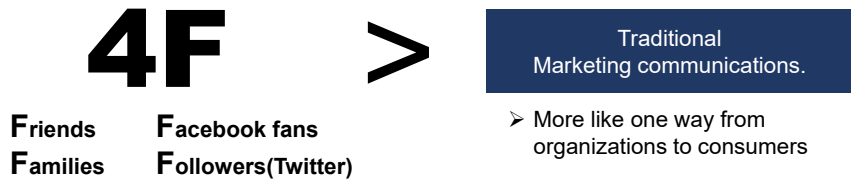
5A by Philip Kotler



Both of B2C / B2B

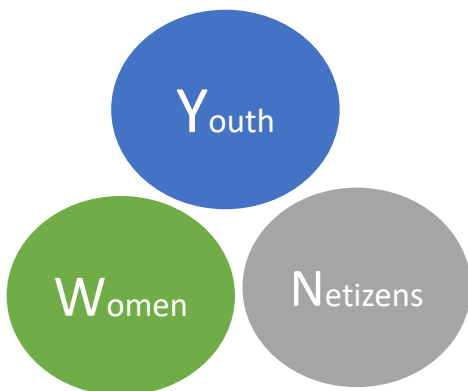
(2) Trusted source

More people believe in 4Fs more than traditional marketing communication.



(3) Key Segment

YMN are the key segments in the digital era.



Youth:

- Early adopters of new products / technologies.
- Trend setters

Women

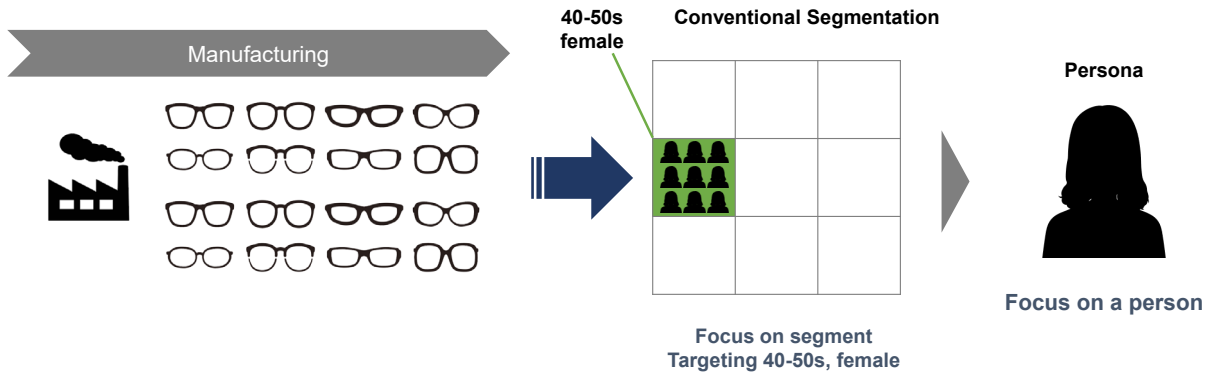
- Information collectors
- Holistic shoppers
- De facto household managers,
- CFO
- Asset manager

Netizens


- Social connectors (overwhelmingly connect, converse, and communicate with their peers)
- Expressive evangelists
- Content contributors in the online world.

10.4.3 Persona Marketing

Conventional STP analysis is sometimes not enough for precise targeting in a way. Segmentation has been linked more to “a group” than “a person”. But it is now important to identity a persona to understand your target audience more specifically.



Persona: A profile that represents your target audience



Hanako Suzuki

■ **Family**

Husband	Business Board Member (always working late)
Daughter	University Student (3 rd year) Living with family
Son	University Student (1 st year) Living by himself

■ **Work life**

Occupation	White collar
Title	Manger
Payroll	\$6,000/month
Wake-up time	7:00
Commuting	40 minutes by train Always reading books
Working hours	10:00 – 17:00 *She is the one who always comes to the office first and leave the office first.
Her reputation	Collogues respect her as professional

■ **General Info**

Gender	Female
Age	45
Location	Tokyo
Education	Tokyo University

■ **Lifestyle**

Hobby	Traveling, Reading books, shopping
Interest	Nature, CSR
Motto	where there is a will there is a way

■ **Description**

She used to love luxury brand such as lux Vuitton, Gucci etc. However, she in no more interested in these brands and her interest is more storyteller-products especially the eco products. She participate in Green-activities. She feels stressful when she has not time to read books.

Figure-36 Example of a Persona

Benefits of creating a persona

It helps you develop more precise customer-centric strategy.

- Understanding your customer more precisely
- Easier communication internally
- More pinpointed and aligned marketing mix

10.4.4 Customer Journey Map

It is a diagram that illustrates the steps your customer(s) go through in engaging with your company, whether it be a product, an online experience, retail experience, a service, or any combination.

“Customer Journey map is a diagram that illustrates the steps your customer(s) go through in engaging with your company, whether it be a product, an online experience, retail experience, or a service, or any combination.”

“80% of senior-ranked marketers state that a cohesive customer journey is absolutely critical for success”

Source: Digital marketing Institute (statistics from Salesforce), Adam Richardson (Harvard Business Review)

Case: Bag manufacturer created CJM for their expected customers.

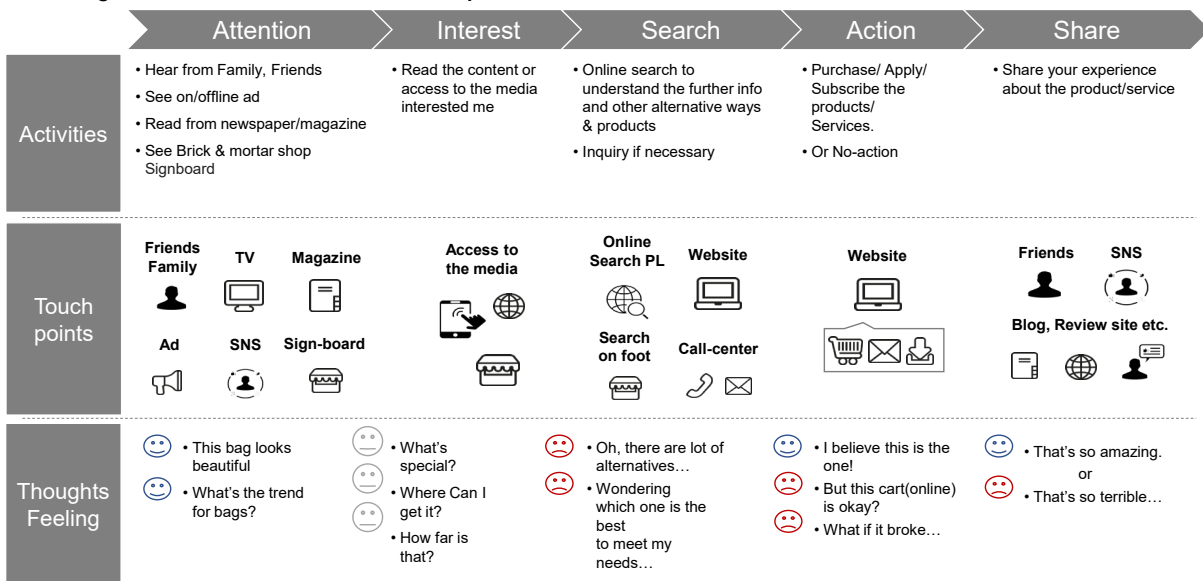


Figure-37 Example of Customer Journey map

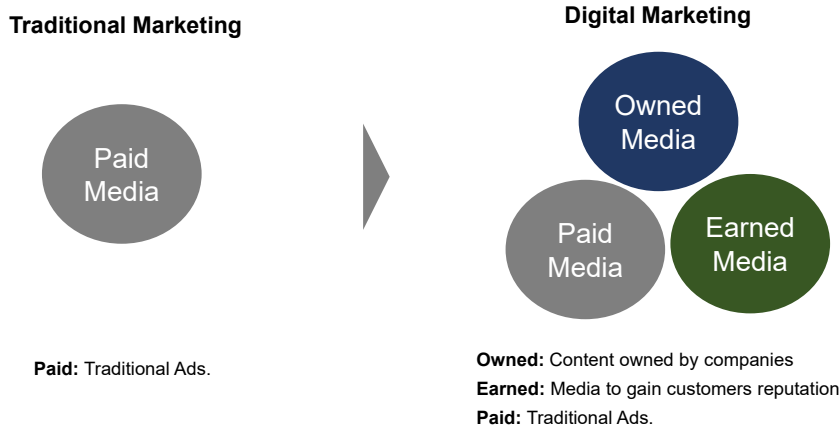
Benefits of creating a customer journey map

It helps you create customer-centric strategy - appropriate touchpoints with appropriate ways (*incl. content)

- Understanding your customer behaviors in the digital era
- Becoming more customer-centric approaches
- Easier communication internally

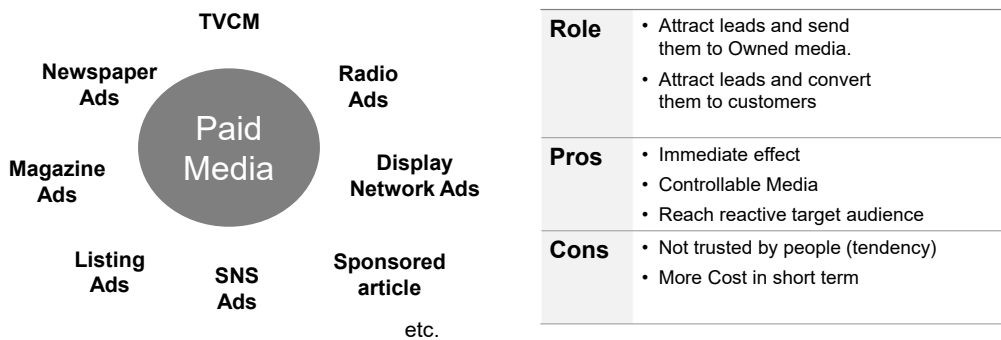
10.4.5 Change of Communication in Digital Era

Not only Paid media, but also owned & earned media are added for digital marketing.



(1) Paid Media

Traditional paid media (such as shown below) become less important in digital marketing.

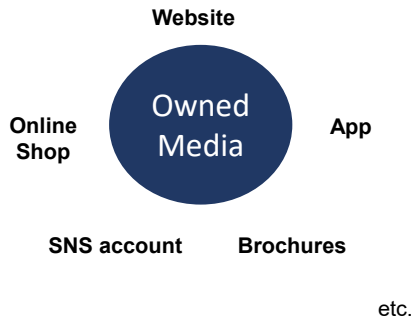


Examples of paid media in digital marketing are:

- Search engine ads/Display ads/Sponsored article/Social media ads

(2) Owned Media

Owned media is the media owned by the company or organization itself and disseminated to consumers, such as PR magazines, pamphlets, and catalogs published by the company, and its own website and blog on the internet. Since it is owned, it is controllable media. It becomes relatively more important.

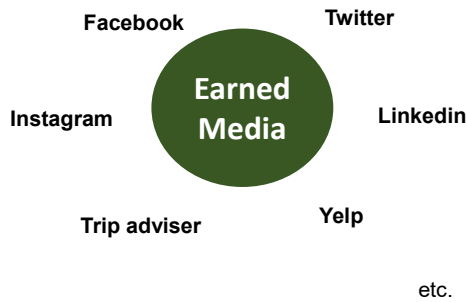


Role	<ul style="list-style-type: none"> • Getting leads • Converting leads to customers • Interaction with earned media
Pros	<ul style="list-style-type: none"> • Controllable Media • Basically, no expenses for Ads • Effect is expected to last longer than traditional Ads if created well.
Cons	<ul style="list-style-type: none"> • Taking longer time to get leads compared to traditional Ads

(3) Earned Media

Earned media is the customer-initiative media. It becomes more important in the digital era.

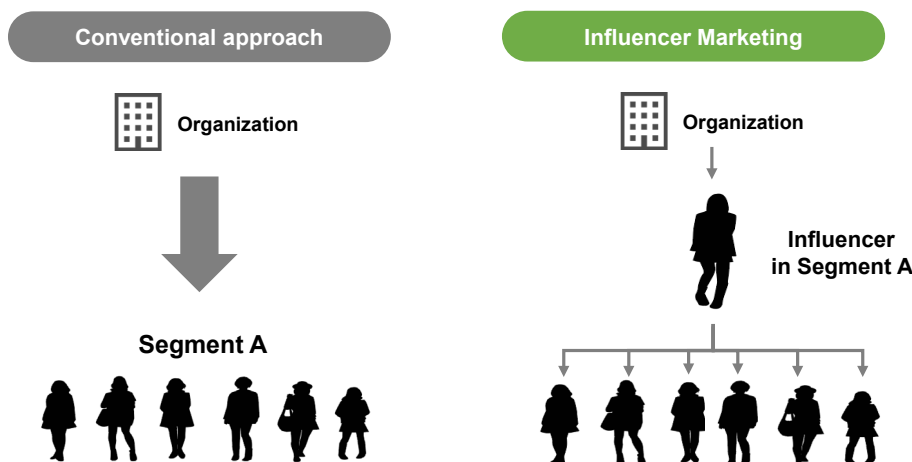
About Earned Media
(Mainly SNS / Review online-platform)
*Not your account



Role	<ul style="list-style-type: none"> • Listening to customers and responding to them
Pros	<ul style="list-style-type: none"> • Transparent • Trusted
Cons	<ul style="list-style-type: none"> • Uncontrollable Media • Taking longer time to get leads compared to Owned media and Paid media.

(4) Influencer Marketing

It is to make a contract with people who have larger impact on specific segments and let them post (for paid/earned media).



There are several types of influencers.

- Celebrities/Bloggers/Instagrammers/YouTubers/Professionals/Authorized media, etc.

(5) Triple Media Strategy - Tips

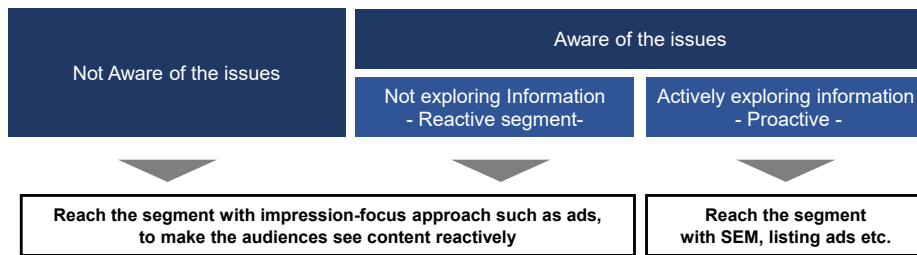
Tips #1: Where is your target audience?

Understanding diversification of people’s online/offline behavior is a key factor to reach your target.



Tips #2: Proactive or Reactive?

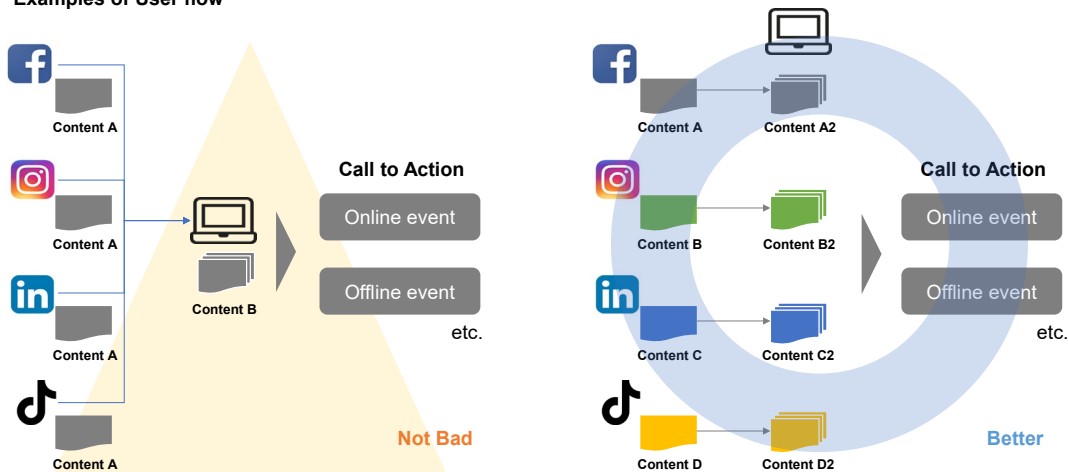
Approaches differ for those who are aware and actively explore, those who are aware but do not explore, and those who are not aware.



Tips #3: Are they right content?

Content needs to be aligned with target audiences’ touchpoints.

Examples of User flow



*The above depends on your objective, resources etc.

10.4.6 Change of System/Database in Digital Era

Digital systems are the key for today's digital marketing. They make business more quantitative and effective.

DSP	Demand side Platform: Advertiser campaign management system ➤Buying ad placements online in real time and distribute them when Advertiser's target user visits a specific website.
MA	Marketing Automation: ➤Providing suitable content to suitable potential customers/customers in suitable timing.
CMS	Content Management System: ➤Opensource software that can be used to create and manage digital content such as WordPress.
SNS	System for Social networking service: ➤System for Social listening and manage/post content for SNS.
CRM	Customer Relation Management: ➤Managing customer attribute, order history etc. by using customer database to optimize one-to-one marketing.
DMP	Data Management Platform: ➤System for managing, analyzing and using customer data

Source: modified Digital Marketing; 10 theories to lead success (Dentsu Digital)

11. How to Measure the Effectiveness of Awareness Raising Activities

As discussed in 10.3.4, setting up appropriate and effective KGI/KPIs is the most important method for measuring the effectiveness of awareness raising activities. KGI/KPI setting should not be done after implementing the target awareness raising activities, but should be conducted from the beginning when developing a strategy for the activity (i.e., the first things to do) because you should set the “Goal” of activity at the beginning.

Once appropriate KGI/KPIs are defined, there are the following methods and metrics that collect the raw data for evaluation.

Table-17 Methods for Collecting Raw Data for Evaluation of Awareness Raising Activities

Activity	Methods/Metrics for evaluation
Physical events	Poll/Questionnaire/Interview
Seminars/Lectures	Questionnaire/Interview
Online videos	Number of views/Percentage of video duration that is played by a viewer/User review/User votes (Up/Down)
Online contents (Web, blog, SNS, etc.)	Number of visits/Number of leached persons (by ad)/Number of clicks on the ad/Online questionnaire/Online interview/Time duration of stay at the content/User review/User votes (Up/Down)

12. Recommendations for Awareness Raising Activities in Vietnam

In this section, we summarize the essence, especially from the viewpoint of awareness raising activities based on the public relations perspective by the public sector rather than the private sector, and keeping in mind that the theme is cybersecurity.

12.1 Learn from experiences in Japan

This report contains many examples of awareness raising activities in Japan, but not all of them have been successful. For example, various videos created by NPA on YouTube achieved very few numbers of views (hundreds at most). On the other hand, a few online videos that collaborated with influencers gained far more accesses. So, it is recommended to carefully examine the results of awareness raising activities in Japan and try to learn what were their success/failure factors. By analyzing these, you can apply only the successful factors/experiences of Japan to your awareness raising activities.

12.2 Setting the target segment in a time frame, but eventually carrying it out to the level where the entire nation is aware of it.

It is undesirable from the viewpoint of fairness that initiatives are allocated to a specific segment because public sector initiatives are based on tax, and also, cybersecurity matters for all citizens. It is necessary to design initiatives with a view to raising awareness fairly among all citizens, including budget allocation. However, from the perspective of achieving effective awareness raising activities, it should be noted that activities should be conducted for each target segment as mentioned earlier when implementing the initiatives.

12.3 Planning content that can involve earned media (third parties)

The level of public awareness/interest in cybersecurity varies depending on demographic attributes and literacy, which means it is not easy for all citizens to take an interest in cybersecurity. Therefore, it is important to design content that earned media such as newspapers, TV etc. can proactively.

12.4 Inducing synergy effects in awareness raising activities by bundling cybersecurity initiatives with other IT-related initiatives

Various initiatives that focus only on cybersecurity may not motivate people to watch or participate as much as expected because of their demographic attributes and literacy as mentioned earlier. Thus, the number of reaches might become lower. It can be said that would happen as well for companies and organizations in the private sector, where cybersecurity is self-evidently important. That is likely to depend on the size of their companies/organizations. On the other hand, there are certain demands for applying for government subsidies due to the benefits of funding for companies. In view of the above two points, it is effective to bundle cybersecurity initiatives such as conducting online self-diagnosis of cybersecurity, creating IT operation policies, etc. with other IT-related subsidies for productivity improvement, etc. That increases the number of companies that can recognize and understand the importance of cybersecurity. This kind of scheme is highly recommended to achieve a wider reach.

12.5 Setting indicators that can be monitored at fixed points

From the operational point of view, it is obviously important to set up indicators for fixed-point observation after conducting awareness raising activities, but it is also significantly important to conduct

surveys using the set indicators to set a standard value before the awareness raising activities so that evaluating and improving the initiatives appropriately becomes possible. In setting indicators, it is important to conduct not only the conventional questionnaire survey but also social listening (online) due to the characteristics of cybersecurity and the penetration of the internet and smartphones. It is also important to verify the set indicators and targeted figures every year, rather than just setting them once.

12.6 Improving the cybersecurity literacy of government officials (including those in local governments)

In the public sector, while certain departments such as the public relations department oversees awareness raising activities, government (including local government) employees are the ones who usually communicate with citizens. Therefore, it is important for administrative staff members, including those in ministries and local governments, to understand the importance of cybersecurity and to be able to correctly convey the message whenever necessary, rather than considering the awareness raising activities such as seminars, content distribution conducted by specific departments are nothing to do with themselves. It is also important from the branding perspective to enhance the perceived quality from citizens to gain the public trust. For this purpose, it is essential to provide internal training to improve cybersecurity literacy with the administrative staffs including those in local governments.

(End of Document)

Appendix 1: Worksheets for STP Analysis

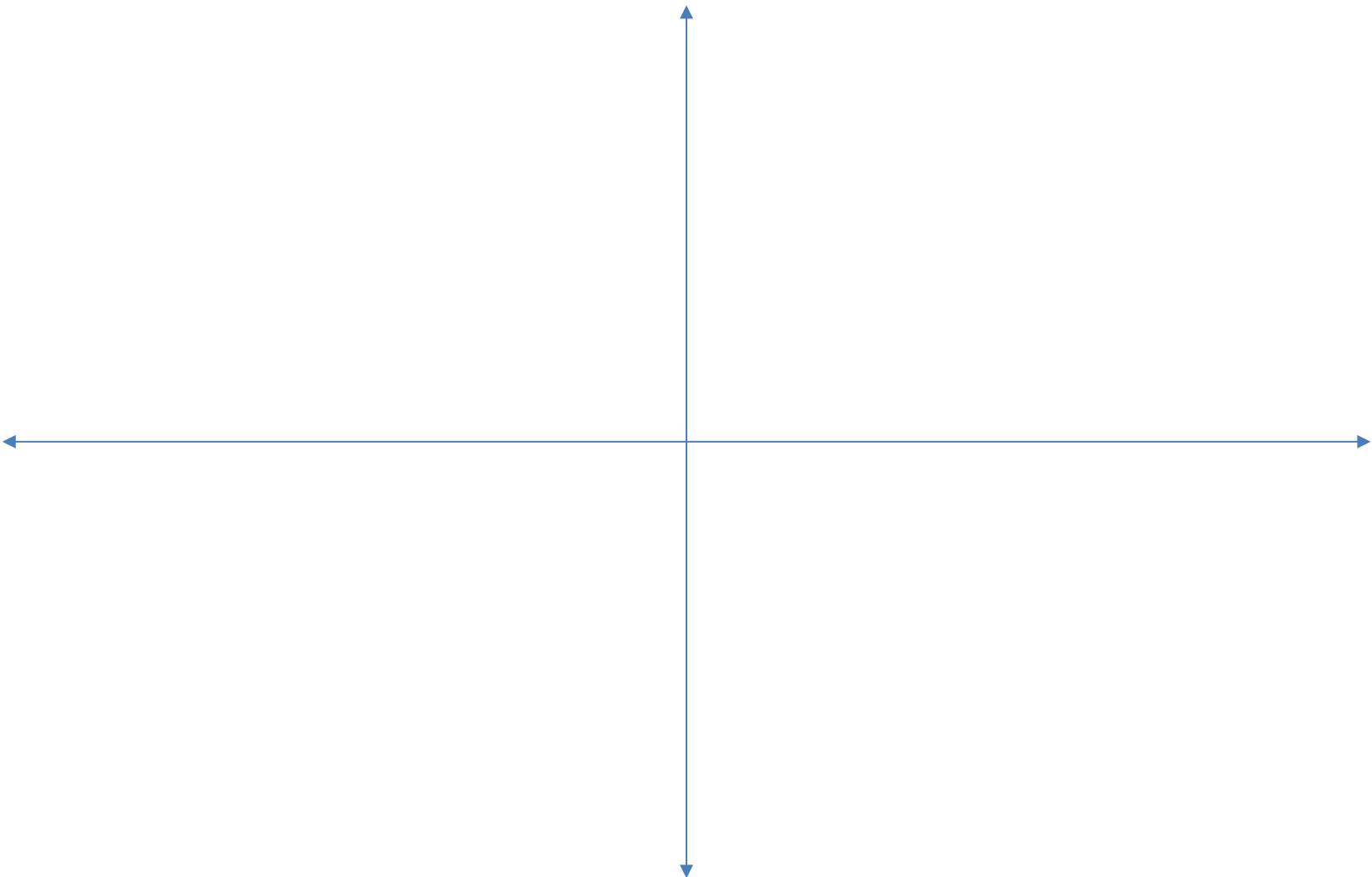
Worksheet for Segmentation:

*It doesn't have to be four quadrants. It depends on your project.

Worksheet for Targeting:

Criteria				
1				
2				
3				
4				
5				
6				

Worksheet for Positioning Map:



Worksheet for Positioning (Feasibility):

Requirement	Feasibility	Cost
-------------	-------------	------

1



2



3



4



Conclusion: