Introduction of Japanese Government Current Policy for Cybersecurity Research and Development

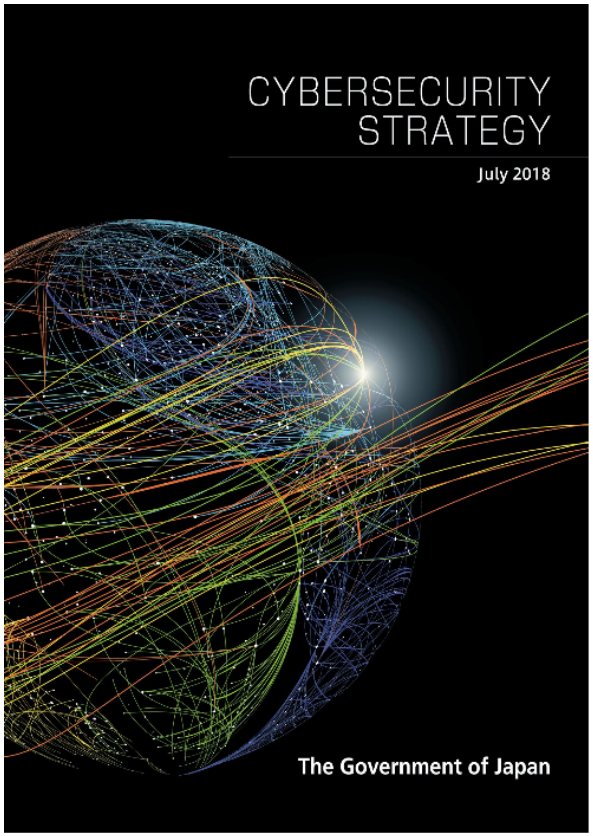
UEDA Mitsuyuki
Counsellor, Strategy and Policy Planning
Nacional center of Incident readiness and Strategy for Cybersecurity(NISC),
Cabinet Secretariat, Government of Japan

February 25, 2021

Cybersecurity Strategy

Cabinet Decision /
Cybersecurity Strategic HQ
July 2018

- Formulated in 2018, it articulates the goals, principles, philosophy, and approaches of Japan's cybersecurity policy for three years.
- Research and development promotion is described as "a foundation for the policy goals from both a cross-cutting perspective and mid- and long-term perspectives."




CONTENTS

As the unification of cyberspace and real space continues, practical research and development (R&D) on cybersecurity is needed, given the advancement of innovation in cyberspace and the threat of cyberattacks against those innovations. Along with this, responses with a view to discontinuous evolution of technology and society over the mid-and long-term are also necessary.

Excerpted from 4.4

Cybersecurity Research and Technological Development Initiative Policy

R&D Strategy Expert Panel,
Cybersecurity Strategic HQ
May 2019

Following *Cybersecurity Strategy*, it articulates the initiative policy for the government's efforts for the promotion of research and technological development.

Directions of strengthening efforts

1. Technical verification for supply chain risk (SCR)

- Technology to check vulnerabilities and malicious functions of ICT equipments and devices.
- Organize technical verification implementation framework of public-private partnership.

[NISC, METI, MIC, CAO]

2. Development of domestic industry

- Establish a comprehensive verification infrastructure to create, utilize, and verify the reliability of cybersecurity products and services originated in Japan to promote "Proven in Japan".
- Support for business creation to meet the needs of small and medium enterprises. (Cybersecurity Help Team, etc.)

[METI]

3. Attack detection, analysis, and sharing infrastructure

- Advance observation technology for quick detection of cyber attacks, and use AI and other technologies to advance efficiency and automation of analysis. (NICTER, STARDUST, etc.)
- Build an infrastructure (CURE) for sharing cyber attack detection and analysis data.

[MIC, METI]

4. Research on cryptography and related area

- Security technologies in future such as post-quantum cryptography and quantum cryptography, and research and development of cryptographic technologies that can be used in IoT devices.

[MIC, METI]

5. Industry, academia, and public sector collaboration

- Community formation among industry, academia, and public sector.

[NISC]

(tentative translation of outlines)

A current discussion of a WG on the promotion of cybersecurity research and industry-academia collaboration

- ✓ Established in July 2020 under *R&D Strategy Expert Panel* (chair: Prof. MATSUMOTO Tsutomu, Yokohama National University) of Cybersecurity Strategic HQ

- ✓ WG members:

(chair)	MORI Tatsuya	Waseda Univ.
	AKIYAMA Mitsuaki	NTT Secure Platform Laboratories
	ARAKI Shoko	Soliton Systems
	HOMMA Naofumi	Tohoku Univ.
	NAGAYAMA Shota	Mercali
	SUGA Yuji	Internet Initiative Japan
	TAKAHASHI Kenta	Hitachi
	YAMADA Akira	KDDI Research
	YAMAUCHI Toshihiro	Okayama Univ.
	YOSHIOKA Katsunari	Yokohama National University

Recent trend of research papers

- A total of 435 papers have been presented at the four conferences (IEEE S&P, ACM CCS, USENIX Security, NDSS) in 2019*.
- The percentage of internationally co-authored papers is 43%, the percentage of industry-academia collaboration papers is 20%, and 5 papers involve Japanese research institutions. (2018: 2 papers, 2014: 2 papers)

Ex) USENIX Security → China is making strides. The number of papers on industry-academia collaboration is increasing.

2014年

分数カウント

Ranking	Country	# Papers	Share
1	アメリカ US	46.73	69.7%
2	ドイツ DE	10.35	15.4%
3	カナダ CA	2.11	3.1%
4	イスラエル IL	1.67	2.5%
5	中国 CN	1.13	1.7%
6	フランス FR	1.00	1.5%
6	スイス CH	1.00	1.5%
6	オーストラリ AU	1.00	1.5%
9	オランダ NL	0.65	1.0%
10	ハンガリー HU	0.50	0.7%
11	シンガポー SG	0.33	0.5%
12	ギリシャ GR	0.20	0.3%
12	サウジアラ SA	0.20	0.3%
14	アルゼンチン	0.14	0.2%

Total # of papers 67本

Internationally co-authored	19本	28%
Industry-academia collaboration	15本	22%

Microsoft 6本, Intel 2, RSA 2, Google 1, SAP 1, NEC米 1 等

2018年

分数カウント

Ranking	Country	# Papers	Share
1	アメリカ US	60.44	60.4%
2	ドイツ DE	12.28	12.3%
3	中国 CN	5.77	5.8%
4	イギリス GB	3.33	3.3%
5	オランダ NL	3.08	3.1%
6	カナダ CA	2.14	2.1%
6	フランス FR	2.08	2.1%
8	スイス CH	1.60	1.6%
9	ベルギー BE	1.43	1.4%
10	フィンランド FI	1.17	1.2%
11	イタリア IT	1.07	1.1%
12	スペイン ES	1.00	1.0%
12	ポルトガル PT	1.00	1.0%
12	イスラエル IL	1.00	1.0%
12	韓国 KR	1.00	1.0%
16	オーストリア	0.50	0.5%
17	ポーランド	0.40	0.4%
18	ルクセンブルク	0.33	0.3%
19	チェコ	0.20	0.2%
20	オーストラリア	0.18	0.2%

Total # of papers 100本

Internationally co-authored	28本	28%
Industry-academia collaboration	19本	19%

Google 4本, Microsoft 2, Symantec 2, IBM 1, Samsung 1, Huawei 1, NEC米 1, Cisco 1, Siemens 1, GE 1 等

2019年

分数カウント

Ranking	Country	# Papers	Share
1	アメリカ US	59.42	52.6%
2	ドイツ DE	13.34	11.8%
3	中国 CN	9.62	8.5%
4	イギリス GB	7.38	6.5%
5	オランダ NL	3.81	3.4%
6	スイス CH	3.67	3.2%
7	イスラエル IL	3.27	2.9%
8	韓国 KR	2.14	1.9%
9	オーストリア AT	2.07	1.8%
10	シンガポー SG	1.78	1.6%
11	フランス FR	1.14	1.0%
12	日本 JP	1.00	0.9%
12	フィンランド FI	1.00	0.9%
12	ルクセンブル LU	1.00	0.9%
15	イタリア	0.79	0.7%
16	チェコ	0.50	0.4%
17	ベルギー	0.32	0.3%
18	オーストラリア	0.29	0.3%
19	スペイン	0.22	0.2%
20	サウジアラビア	0.14	0.1%
21	カナダ	0.08	0.1%

Total # of papers 113本

Internationally co-authored	48本	42%
Industry-academia collaboration	30本	27%

Microsoft 3本, Symantec 3, Google 2(+2), IBM 2, Samsung 2, Baidu 2, Barracuda NW 2, Intel 1, Huawei 1, NEC米 1, NEC独 1 等 ()内は単独論文

(*) NISC compiled the data from the website information, taking into account the affiliation of each author.

Recent trend of research papers（Crypto）

- The cryptography research trend tends to differ from the four conferences. A certain presence of Japan is observed.
- The largest number of Japanese research institutes participated in is NTT (Nippon Telegraph and Telephone Corporation).

Ex) Crypto → <u>The number of papers on industry-academia collaboration is increasing.</u>

2014年

分数カウント

Ranking	Country	# Papers	Share
1	アメリカ US	25.03	42.4%
2	イスラエル IL	7.25	12.3%
3	ドイツ DE	4.07	6.9%
4	日本 JP	3.75	6.4%
5	フランス FR	2.98	5.1%
6	イギリス GB	2.42	4.1%
7	中国 CN	2.15	3.6%
8	シンガポール	1.75	3.0%
9	スイス	1.08	1.8%
9	スペイン	1.08	1.8%
11	インド	1.00	1.7%
11	エストニア	1.00	1.7%
11	オーストリア	1.00	1.7%
14	韓国	0.95	1.6%
15	不明	0.67	1.1%
16	デンマーク	0.58	1.0%
17	オランダ	0.50	0.8%
18	カナダ	0.33	0.6%
18	イタリア	0.33	0.6%
20	オーストラリア	0.25	0.4%
20	ベルギー	0.25	0.4%
22	スウェーデン	0.20	0.3%
22	台湾	0.20	0.3%
22	マケドニア	0.17	0.3%

Total # of papers 59本

Internationally co-authored	32本	54%
Industry-academia collaboration	13本	22%

IBM 4本, NTT 3, Microsoft 3 等

2018年

分数カウント

Ranking	Country	# Papers	Share
1	アメリカ US	33.44	42.3%
2	イスラエル IL	9.05	11.5%
3	フランス FR	5.65	7.2%
4	ドイツ DE	4.83	6.1%
5	デンマーク DK	3.68	4.7%
6	日本 JP	3.63	4.6%
7	イギリス GB	3.16	4.0%
8	インド IN	3.08	3.9%
9	中国	2.59	3.3%
10	シンガポール	1.58	2.0%
11	ベルギー	1.27	1.6%
12	韓国	1.14	1.4%
13	スイス	0.95	1.2%
13	イタリア	0.95	1.2%
15	オランダ	0.70	0.9%
16	オーストリア	0.63	0.8%
17	イラン	0.57	0.7%
18	ノルウェー	0.50	0.6%
18	ポルトガル	0.50	0.6%
20	オーストラリア	0.33	0.4%
21	ルクセンブルク	0.31	0.4%
22	チェコ	0.25	0.3%
23	スペイン	0.20	0.3%

Total # of papers 79本

Internationally co-authored	43本	54%
Industry-academia collaboration	16本	20%

NTT 5本, IBM 4, Microsoft 2, Visa 1 等

2019年

分数カウント

Ranking	Country	# Papers	Share
1	アメリカ US	39.05	48.5%
2	イスラエル IL	6.19	7.7%
3	日本 JP	4.53	5.6%
3	中国 CN	4.53	5.6%
5	デンマーク DK	3.60	4.5%
6	ドイツ DE	3.46	4.3%
7	フランス FR	3.30	4.1%
8	オランダ	3.08	3.8%
9	イギリス	1.72	2.1%
10	インド	1.45	1.8%
11	イタリア	1.40	1.7%
12	ベルギー	1.23	1.5%
13	カナダ	1.20	1.5%
14	スイス	1.13	1.4%
15	オーストラリア	1.00	1.2%
16	韓国	0.80	1.0%
17	シンガポール	0.63	0.8%
18	スペイン	0.50	0.6%
18	イラン	0.50	0.6%
20	ラトビア	0.33	0.4%
20	エストニア	0.33	0.4%
22	台湾	0.25	0.3%
23	ノルウェー	0.20	0.2%
24	オーストリア	0.08	0.1%

Total # of papers 81本

Internationally co-authored	44本	54%
Industry-academia collaboration	23本	28%

NTT 4本, Microsoft 4, NTT米 3, IBM 1, Visa 1, Qualcomm 1, Deepmind 1, Fujitsu米 1, NEC 1 等

（*）NISC compiled the data from the website information, taking into account the affiliation of each author.

Cybersecurity research and industry-academia-public sector collaboration strategy WG Interim Report (summary)

R&D Strategy Expert Panel's WG
Cybersecurity Strategic HQ
October 2020

～Establishing an ecosystem across industry, academia and public sector to boost international competitiveness in R&D～

Chap.1 Introduction

Youthful and growing research field

- Paper submissions to top international conferences more than quadrupled compared to 2000.
- In Japan as well, the number of participants in major research meetings has more than doubled in the 2010s.

Very active in collaborations

- The number of internationally co-authored papers and industry-academia-public sector collaboration papers is increasing internationally.
- As security measures need to be integrated with digital tech advancement, academic research on security is considered one of the main engines of wealth and vitality.

▷ **Now is a critical time to building an ecosystem across industry, academia and public sector.**
／ Need to proceed in parallel with digitalization in Japan

Chap.2 Promotion measures based on the situation of research community in Japan

▷ **Building a cycle for driving the ecosystem**

2.1 International trends and characteristics of the research field

- Doctoral students are paid full-time and are valuable research force.
- In this field, as in the field of information technology, flexible and talented "human resources" can greatly advance the research.
  (Based on computer science, it often involves programming and trial and error.)

2.2 Should invest in "people"

- In the doctoral course, acquisition of knowledge and methodology in the specialized field is fundamental, but a certain amount of real-world experience is also important.
  (Internships, industry-university joint research, etc.)
- Effective utilization of research assistant (RA) expenses and flexibility of upper limit are important.
  (A viewpoint to promote research by welcoming excellent doctoral students as a research force with RA expenses.)
- In research projects and industry-academia joint research funds, RA expenses should be set flexibly, and a form of welcoming excellent personnel is necessary in this field.
  (It enables various doctoral course admission, including people with business experiences.)

2.3 Possibility of industry-academia-public sector collaboration

- With the expansion of cyberspace, there are potentially many partners for academia. Collaborative research projects involving a certain amount of data and/or research funds are expected.
- In Japan as well, industry-academia joint research that invests research funds more in "people" should be considered.

2.4 Further development of the entire research community

- Utilization of funding opportunities and research funds is important.
  (It is important that the situation and trends of the research community are well taken into account in the planning process of the government and funding agencies.)
- Importance of establishing scientific foundations.
  (Scientific foundations can act as verbalization of core concepts of values that the scientific method can provide in collaboration with other fields and the real world.)
- Evaluation of flexible research achievements including proceedings paper.

Chap.3 Japan's strengths and potential and toward focused strengthening

3.1 Japan's strengths and potential

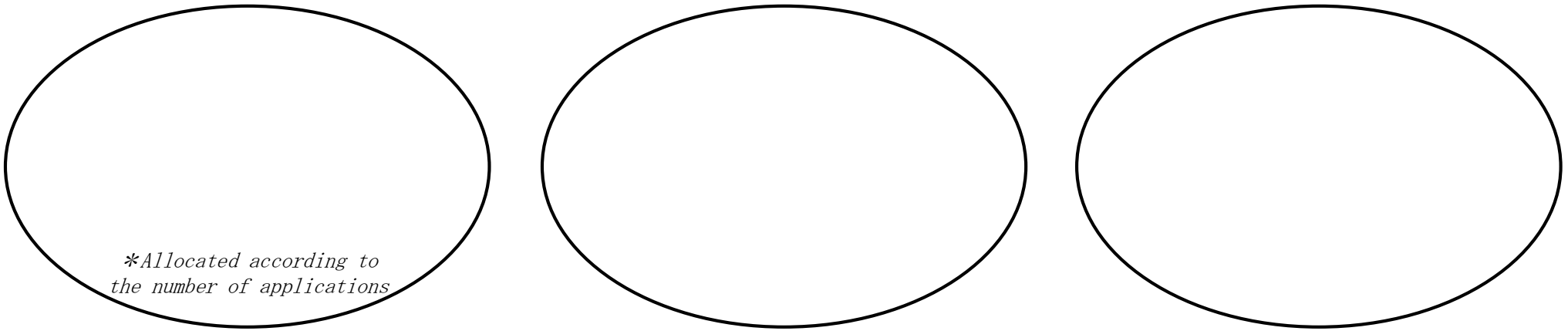
- Research areas such as IoT security, and data security and privacy protection are considered comparable to the U.S. and Europe.
- Research areas related to the fusion of real space and cyberspace in Society 5.0 and research areas that utilize the strengths of cryptography research have strengths in terms of potential.

3.2 Focused research areas (See later slide)

(tentative translation)

Research funding of government funding agencies in Japan

There may be room to further increase the development potential of the research community.



Research based on free ideas

(Bottom-up)

Research & Development in response to policy issues

(Top-down)

Researchers propose research topics freely

JSPS Grants-in-Aid for Scientific Research

Researchers propose research topics under determined research areas

JST funding （CREST / PRESTO, etc.）

Other fundings to promoete Industry-academia collaboration, etc.

Researchers are invited in R&D projects

SIP, MIC, NEDO, etc.

MIC SCOPE

MIC: Ministry of Internal Affairs and Communications
JSPS, JST, NEDO: funding agencies SIP: Cross-ministerial Strategic Innovation Promotion Program (operated by Cabinet Office)

Focused research areas

Following are the research areas which would ideally contribute to the enhancement of intellectual value, and social and economic value. Analysis of strengths and potential is also taken into account. To strengthen academic research, it is desirable for stakeholders to focus on these research areas, being coupled with the self-supporting efforts of the research community.

Safe and secure social infrastructure

Digital Infrastructure (IoT, 5G, Cloud, City OS, etc.) Security

IoT security research area in Japan is considered at a level of strength comparable to that in the U.S. and Europe, and there is further strength in terms of potential due to the development of domestic observation network. The research area on digital infrastructure including IoT should be strengthened.

Supply Chain Security

In this research area, it is considered that the U.S. has strength, followed by Europe and Japan being at almost the same level. Scholarly publication seems underdeveloped even internationally. Since there may be some technologies that are related to various industries and cannot be easily relied on other countries, such as verification technologies for supply chain risks, the research area should be strengthened.

Data Security and Privacy Protection*

This research area in Japan is considered at a level of strength comparable to that in the U.S. and Europe. Data is the source of industrial and social activities and privacy protection is important. The research area should be strengthened.

Implementation Security (including hardware security)*.

It is considered that Europe has particular strength, followed by the U.S., China and Japan being at almost the same level. The research area is related to the implementation stage and the cryptography research where there is an accumulation of knowledge and strength, and it should be strengthened.

Areas to be addressed for the future

AI Security

It is considered that the U.S. has particular strength, second only to Europe, but the trend in research activities and achievements is on an upward trend. As the AI Strategy has been formulated and social implementation progresses, it should be strengthened.

Automotive Cybersecurity

It is considered that the U.S. and Europe have strength, followed by Japan. The automotive industry in Japan is strong internationally, and this area is where a unification of real space and cyberspace technology (Society 5.0) happens, which Japan is focusing on. It is considered to have strengths in terms of potential, and should be strengthened.

Proactive approach to overturn attackers' advantage

Offensive Security Research**
(Gaining insights from an attack perspective)

Research that identifies risks and vulnerabilities from the attackers' perspective and finds countermeasures. Rather than reactive approach that focuses on defense, proactive approach from various angles, from technology to operations and systems, can contribute more to countering evolving attacks, and should be promoted.

Research based on Observation and Analysis of Real Data**

Data-driven approach research based on observation and analysis of real data including attack and damage situations. This research is considered to contribute to understanding correctly and countering threat situations in cyberspace, and should be promoted.

Human Factors in Cybersecurity* (Usable Security)

It is considered that the U.S. and Europe has particular strength, and Japan is at the next level, but the trend in research activities and achievements is on an upward trend. Research on human factors has been conducted in Japan, such as evaluation of user perception, user interface, etc. As Society 5.0 is realized and consideration of human factors will become more necessary, this research area should be strengthened.

- * indicates the research area related to the basic elements, and no mark indicates the research area that has a target field, both of them are discussed in the strengths analysis.
- ** indicates research classified as a cross-sectional method/approach that does not apply to the individual research areas discussed in the strengths analysis.

※The continued promotion of the field of cryptography research and the maintenance and enhancement of its international presence are also very important. In addition, research based on the free ideas of researchers through the Grant-in-Aid for Scientific Research, etc. is very important as sources of ideas, theories, and seeds, and should continue to be promoted.

(tentative translation)

（1）Building an ecosystem across industry, academia, and public sector

- WG discussion

（2）Promotion of practical R&D

- Directions in *Initiative Policy* of 2019

（3）Taking into account medium- and long-term technological trends

- Ex: AI, quantum technology

Thank you very much for your attention!

御清聴ありがとうございました。