International Conference on ASEAN-JAPAN Cybersecurity Community（IC-AJCC）2023

Developing Cybersecurity Human Resource

2023/10/6

Professional University of Information and Management for Innovation
(i-University)
Professor　Toshihiro Hirayama

iU情報経営イノベーション専門職大学
教授　平山 敏弘

All Rights Reserved. Professional University of Information and Management for Innovation

Professor Toshihiro Hirayama

Professional University of Information and Management for Innovation
(i-University)
NPO Japan Network Security Association(JNSA)Director,Education Comittee

【Profile】

Have been experiencing a lot of tasks of system design and build for large-scale distributed systems with a central focus on UNIX since joining an IT company. Worked Web systems and commercial Internet systems, and then moved to the security field. and worked as a security principal director in a consulting company. Currently, professor of professional university.

Also, engage in activities regarding business-academia cooperation education and human resource development through the work such as giving lectures about information security, IT career path, etc. as a part-time lecturer in several universities and graduate schools.

【Award】

In 2013, I received the Information Security Leadership Achievement (ISLA) Asian Award from (ISC)² for his contributions to the development of security in the Asia Pacific region.

All Rights Reserved. Professional University of Information and Management for Innovation

Substance of this speech

In the after-covid-19, further digitalization will be driven by the promotion of remote work and the increase in online meetings without traveling to work. On the other hand, the promotion of digitalization will also make users with low security skills more vulnerable to targeted attacks. Therefore, we are entering an era in which security skills will be widely demanded, not only by security experts, but also by users with low security skills.
In this talk, I will introduce the nurturing of **"Plus Security Human Resources"** using **SecBoK(Security Body of Knowledge),** a Body of Knowledge of Security that originated in Japan.

I hope you will know the words "SecBoK" and “Plus security human resources" in this speech.

All Rights Reserved. Professional University of Information and Management for Innovation

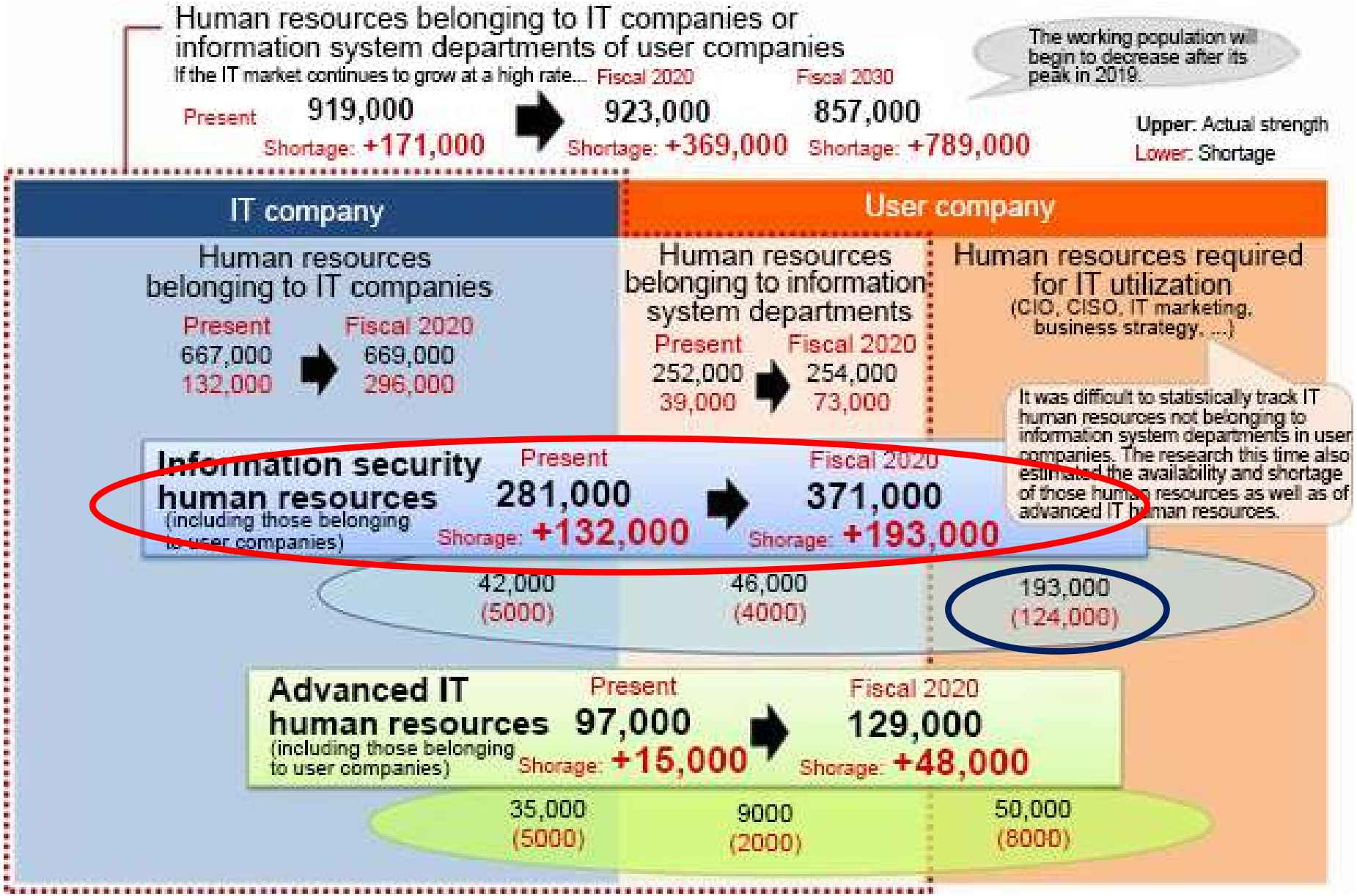
1. Is there really a shortage of Security Human Resources?

All Rights Reserved. Professional University of Information and Management for Innovation

The current shortage of "Security Human Resources" in Japan

All Rights Reserved. Professional University of Information and Management for Innovation

What kind of human resources do we really need? Pay attention to these numbers.

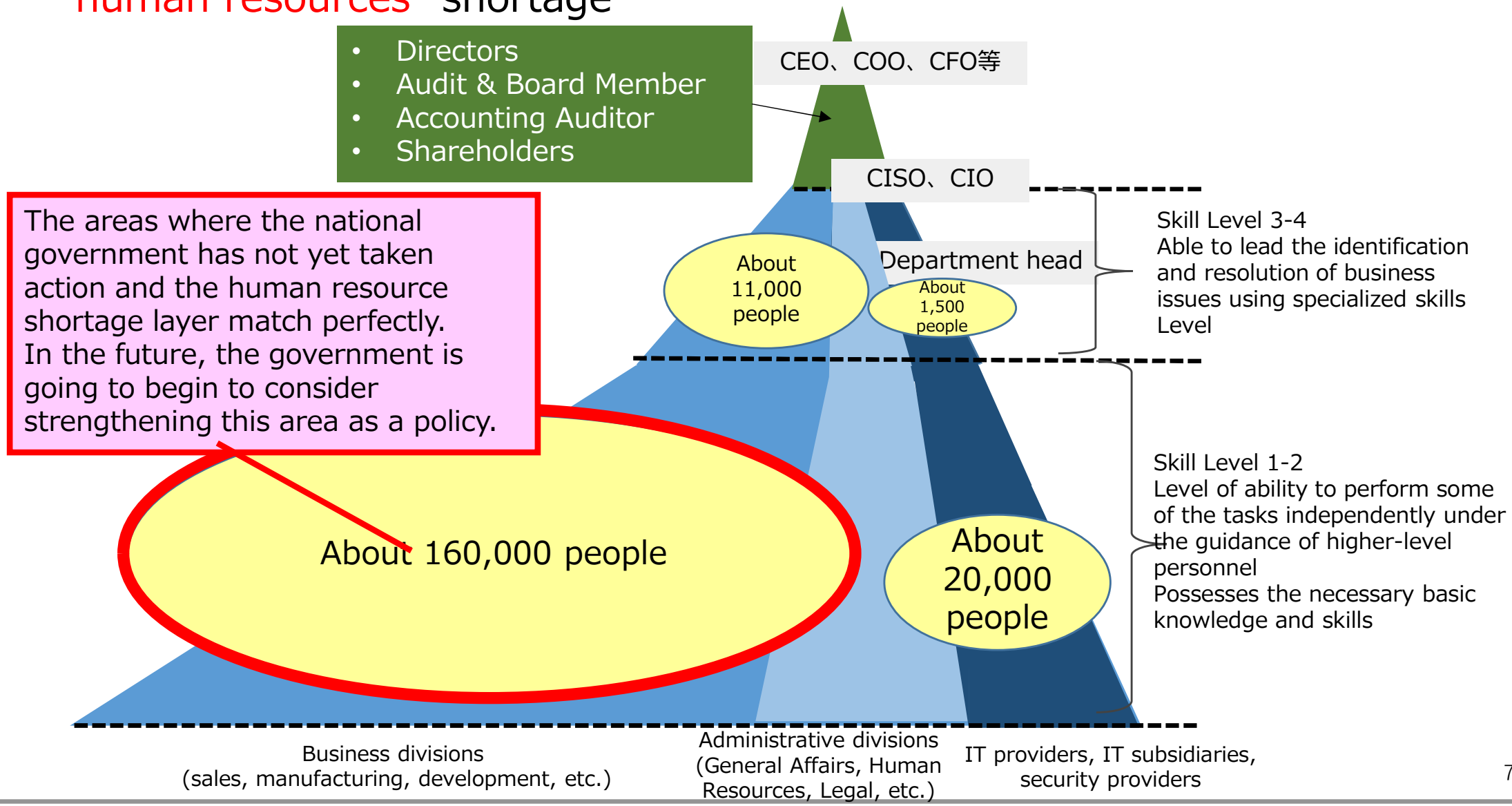


Source: http://www.meti.go.jp/press/2016/06/20160610002/20160610002.html

All Rights Reserved. Professional University of Information and Management for Innovation

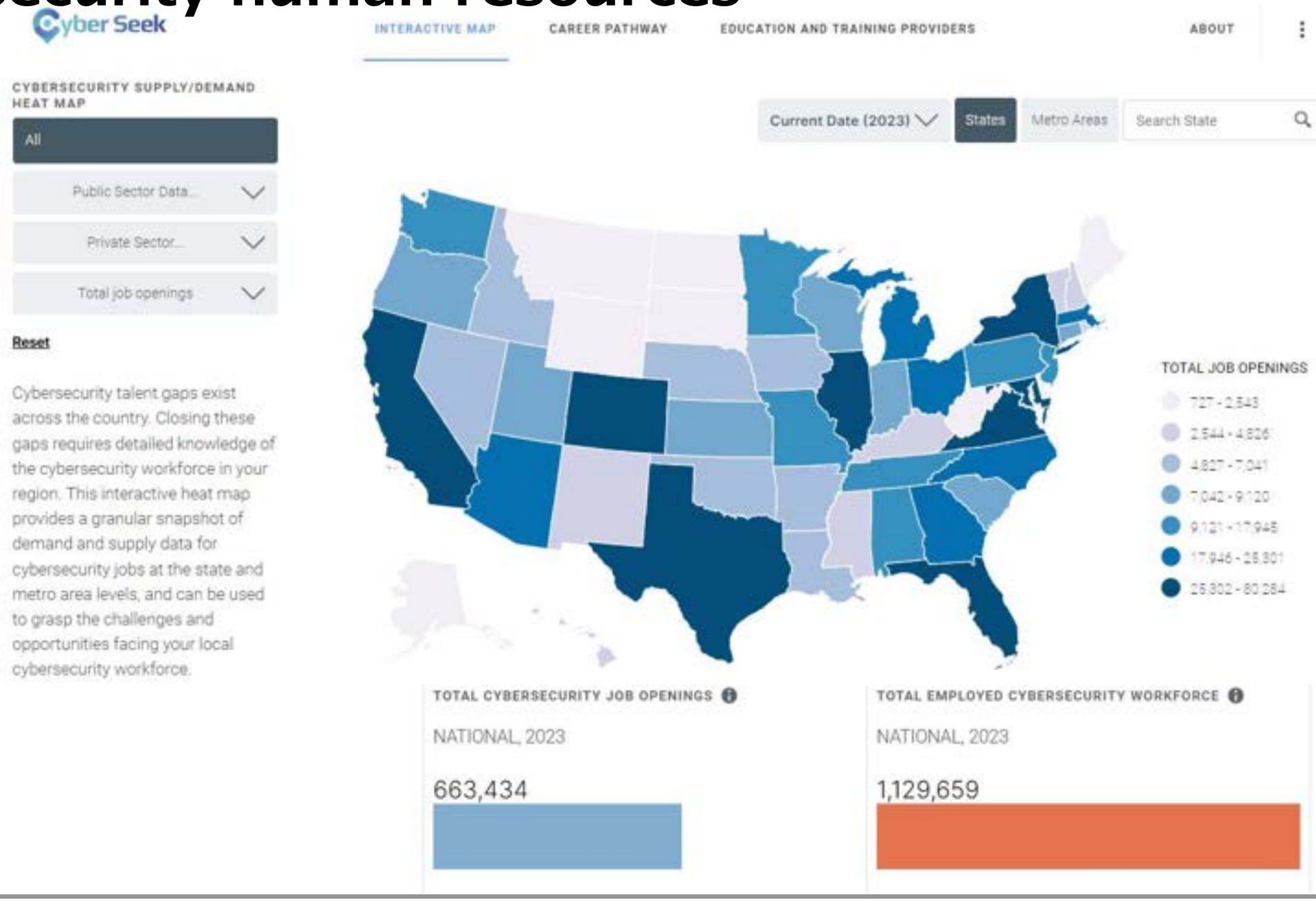
Mapping the number of security human resources shortages

In terms of numbers, it is imperative to address the "plus security human resources" shortage



All Rights Reserved. Professional University of Information and Management for Innovation

Japan is not alone in its lack of security human resources

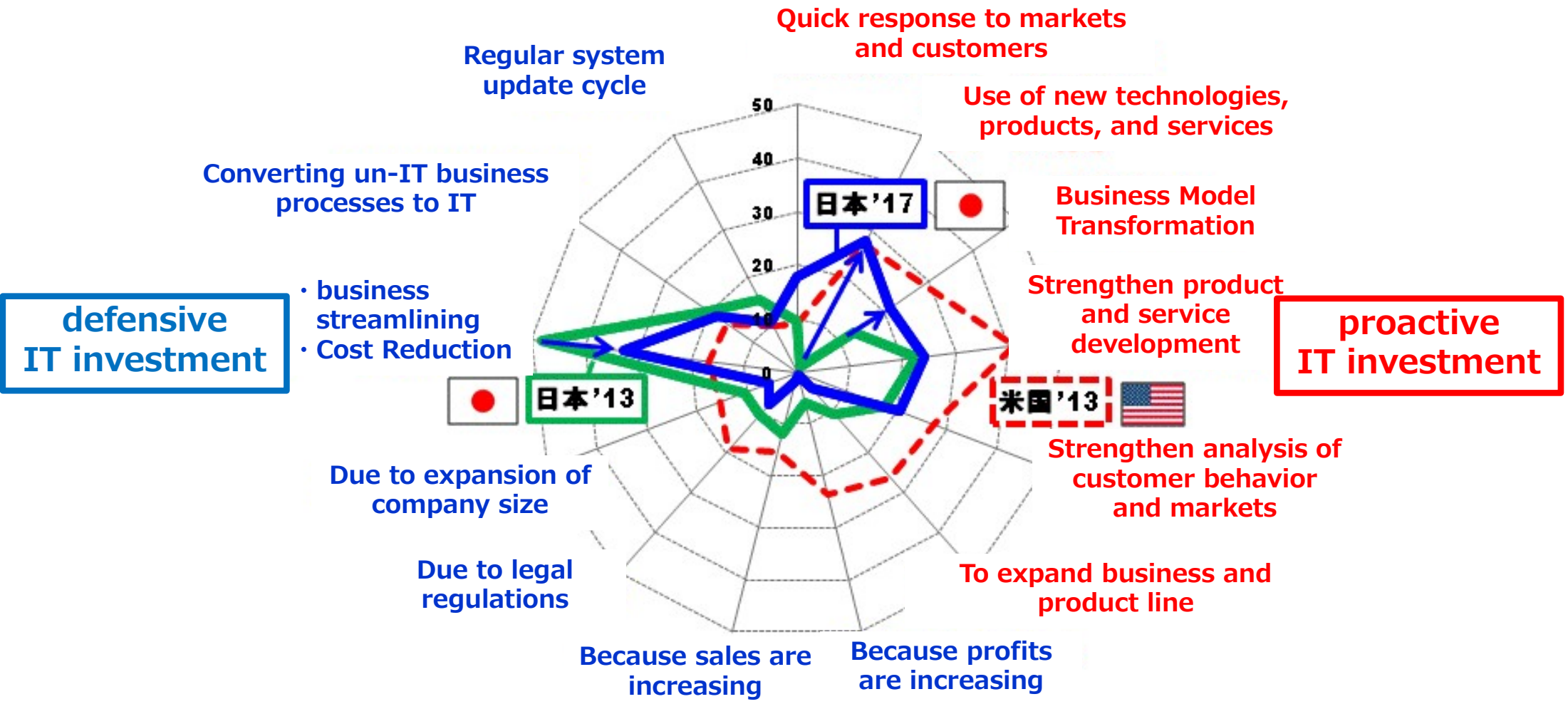


All Rights Reserved. Professional University of Information and Management for Innovation

2. Why is security human resources development so important in Japan?

All Rights Reserved. Professional University of Information and Management for Innovation

From "defensive IT investment" to “Proactive IT investment"



出典：JEITA『2017 年 国内企業の「IT経営」に関する調査結果　https://www.jeita.or.jp/japanese/exhibit/2018/0116.pdf

All Rights Reserved. Professional University of Information and Management for Innovation

Market Capitalization Ranking (1989 vs 2018:Heisei era)

	Company Name	market capitalization (B$)	country		Company Name	market capitalization (B$)	country
1	NTT	1,638.6	Japan	1	Apple	9,409.5	USA
2	The Industrial Bank of Japan	715.9	Japan	2	Amazon	8,800.6	USA
3	Sumitomo Bank	695.9	Japan	3	Alphabet (Google)	8,336.6	USA
4	Fuji Bank	670.8	Japan	4	Microsoft	8,158.4	USA
5	The Dai-Ichi Kangyo Bank	660.9	Japan	5	Facebook	6,092.5	USA
6	IBM	646.5	USA	6	Berkshire Hathaway	4,925.0	USA
7	Mitsubishi Bank	592.7	Japan	7	Alibaba	4,795.8	China
8	Exxon Mobil	549.2	USA	8	Tencent	4,557.3	China
9	Tokyo Electric Power Company	544.6	Japan	9	JPMorgan Chase	3,740.0	USA
10	Royal Dutch Shell	543.6	UK	10	Exxon Mobil	3,446.5	USA
11	Toyota	541.7	Japan	11	Johnson & Johnson	3,375.5	USA
12	GE	493.6	USA	12	Visa	3,143.8	USA
13	Sanwa Bank	492.9	Japan	13	Bank of America	3,016.8	USA
14	Nomura Securities	444.4	Japan	14	Royal Dutch Shell	2,899.7	USA
15	NIPPON Steel	414.8	Japan	15	Industrial and Commercial Bank of China	2,870.7	China
16	AT&T	381.2	USA	16	Samsung	2,842.8	Korea
17	Hitachi	358.2	Japan	17	Wells Fargo	2,735.4	USA
18	Matsushita Electric Industrial	357.0	Japan	18	Walmart	2,598.5	USA
19	Philip Morris	321.4	USA	19	China Construction Bank	2,502.8	China
20	Toshiba	309.1	Japan	20	Nestlé	2,455.2	Swiss

出典：2018年8月20日のダイヤモンドオンライン
「昭和という「レガシー」を引きずった平成30年間の経済停滞を振り返る」

11

All Rights Reserved. Professional University of Information and Management for Innovation

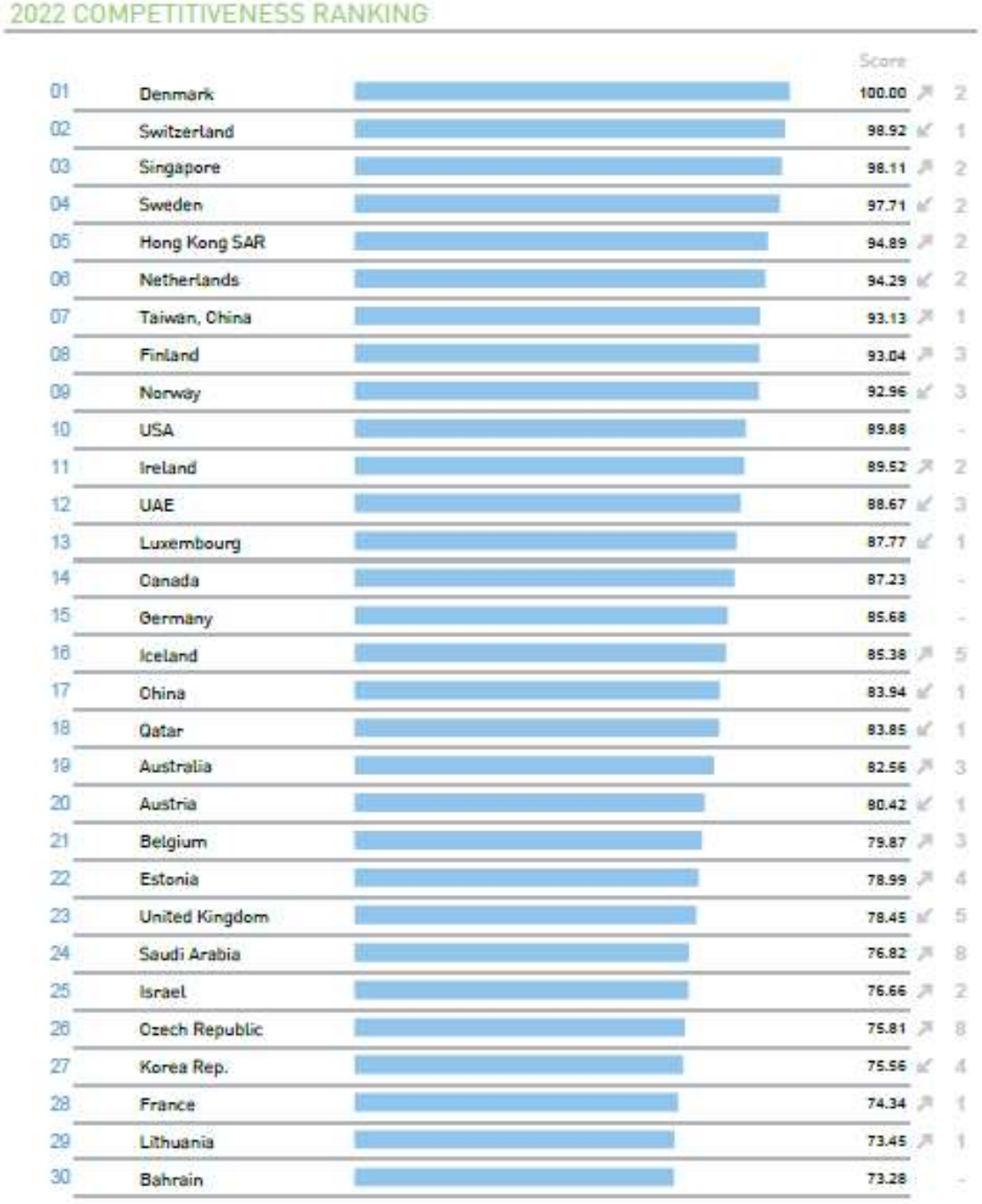
As a result, the difference in market capitalization has finally reached this level

GAFA's total stock market capitalization has exceeded that of all Japanese companies.

According to an August 26, 2021 article in the Nihon Keizai Shimbun, the combined stock market capitalization of GAFA reached $7.05 trillion (about ¥770 trillion), exceeding the $6.86 trillion (about ¥750 trillion) for all Japanese companies. Among GAFAs, Apple has the highest stock market capitalization, with a market capitalization of approximately $2.45 trillion (approximately 267 trillion yen), according to Market Watch. Apple became the first company in history to reach $2 trillion in stock market capitalization since the U.S. stock market opened in August 2020.

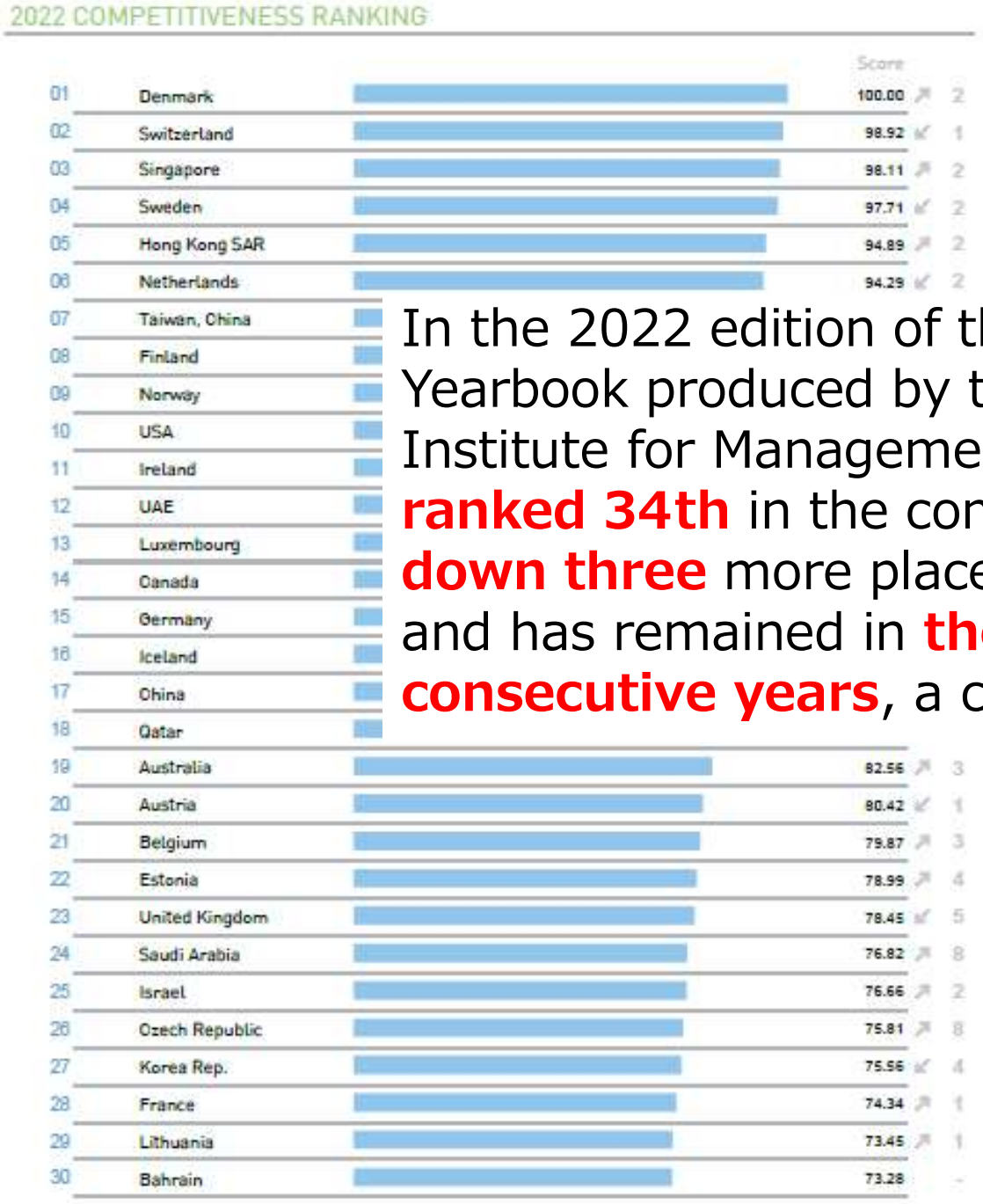
12
All Rights Reserved. Professional University of Information and Management for Innovation

The 2022 IMD World Competitiveness Ranking



All Rights Reserved. Professional University of Information and Management for Innovation

Japan's International Competitiveness in Crisis



In the 2022 edition of the Global Competitiveness Yearbook produced by the IMD (International Institute for Management Development), **Japan is ranked 34th** in the competitiveness ranking, **down three** more places from the previous year, and has remained in **the low 30s for four consecutive years**, a critical situation.

All Rights Reserved. Professional University of Information and Management for Innovation

The 2022 IMD World Talent Ranking

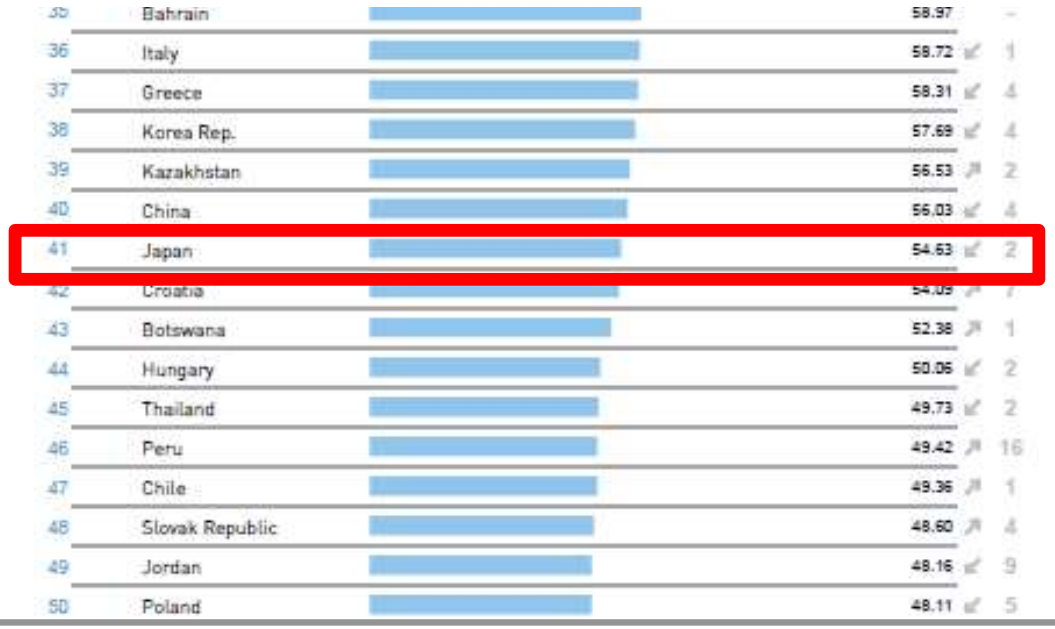
All Rights Reserved. Professional University of Information and Management for Innovation

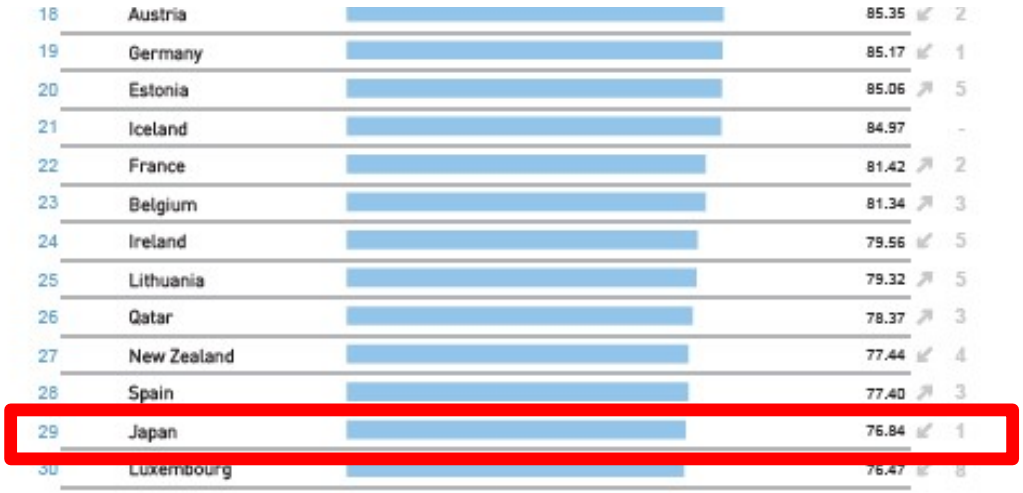
The causes of the lower international competitiveness are "human resources" and "digital"

In particular, in the human resources ranking, **the country is in 41st place**, falling for the fourth consecutive year since 2019, dropping two places from the previous year and stagnating at the bottom of the list among the countries surveyed in recent years.

It also ranks **29th in the Digital Competitiveness Ranking**, a drop of one place from 2021 and the lowest ranking ever since the 2017 survey.

From these results, it is clear that the development of **"digital" + "human resources"** is an urgent necessity in order to increase international competitiveness.





All Rights Reserved. Professional University of Information and Management for Innovation

Security Human Resource Development Essential for Improving International Competitiveness

The IMD report also points out that cybersecurity measures are a top priority for strengthening digital competitiveness, as follows.

World Digital Competitiveness Ranking
https://www.imd.org/centers/wcc/world-competitiveness-center/rankings/world-digital-competitiveness-ranking/

In digitally competitive economies, **cybersecurity measures are top priority** for public and private sector, the 2022 IMD World Digital Competitiveness Ranking also found.

Governments and the private sector need to shield their digital infrastructure **from cyber attacks** if they want to continue in the race for digitally competitive economies. This was **a major finding** in the 2022 edition of the IMD World Digital Competitiveness Ranking, published today by IMD's World Competitiveness Center (WCC).

It is clear **that "human resources" + "digital" + "security"** are necessary to increase international competitiveness, and that it is impossible to **achieve this without "security human resource development".**

Security human resource development is a measure directly related to improving international competitiveness

All Rights Reserved. Professional University of Information and Management for Innovation

Is it clear now for you why “the plus security human resource is lack" is said in Japan?

Data shown by METI* includes prediction and expectation as “it should be”, although it’s true that there’s a lack of security human resources.

↓

In other words, when "security human resoueces development" is further strengthened to increase the competitiveness of "human resources" + "digital" + "security," there will be a significant shortage of "plus security personnel" in the business sector.

↓

The lack of security human resources in US is just at this stage.

*METI: Ministry of Economy, Trade and Industry, Japan

All Rights Reserved. Professional University of Information and Management for Innovation

3. What is the new term “plus security human resources”?

All Rights Reserved. Professional University of Information and Management for Innovation

Security Human Resource Development Policy and Plus Security in Japan

All Rights Reserved. Professional University of Information and Management for Innovation

Cyber Security Strategy 2021
"Plus security" is one of the issues to be considered in Japan

The NISC (National center of Incident readiness and Strategy for Cybersecurity) will launch a new "Next Cyber Security Strategy" in FY2021. One of the cross-sectional measures in the strategy is "securing, developing and promoting human resources", which is taken up as an environment for supplementing "plus security knowledge".

https://www.nisc.go.jp/conference/cs/jinzai/dai13/pdf/13shiryou0103.pdf

1. Establish a new development, monitoring and response system to ensure cyber security.

Consideration of measures to establish and disseminate a new development system and monitoring and response system for rapid and flexible businesses, products, and services that incorporate security.

2. Promote an environment and human resource development that can supplement the "plus security" knowledge required for DX*.

Consideration of measures to promote an environment and human resource development in which those responsible for management and business related to DX can supplement their "plus security" knowledge.

3. Promote liquidity and matching opportunities for cyber security personnel to promote their activities

Consideration of ways to broaden opportunities for security human resources, make career paths more attractive, and promote liquidity and matching opportunities.

*DX: Digital Transformation

All Rights Reserved. Professional University of Information and Management for Innovation

4. Overview of Security Body of Knowledge (SecBoK)

All Rights Reserved. Professional University of Information and Management for Innovation

Development of Information Security Engineers

1) Requested from IPA(Information-technology Promotion Agency, Japan), the Information Security Skill Map was created in 2004 and 2005 (revision).

http://www.ipa.go.jp/security/fy15/reports/skillmap/documents/skillmap_2003.pdf
http://www.ipa.go.jp/security/fy16/reports/skillmap/documents/skillmap_2004.pdf

2) Renamed from JNSA(NPO Japan Network Security Association), SecBoK opened to public as an entrusted business from Ministry of Economy, Trade and Industry.

The knowledge described in the *Guidebook for Instructors of Information Security Education (2007 Edition)* is SecBoK (p. 40 - p. 67).
http://www.jnsa.org/result/2007/edu/materials/071111/tebiki2007.pdf

All Rights Reserved. Professional University of Information and Management for Innovation

What is SecBoK ?　NIST SP800-181 Coordination

SecBoK: Security Body of Knowledge

Over 1,000 skills in NIST SP800-181 were coordinated with 16 roles in SecBoK .
(Category changes, itemization of the basics, general descriptions, etc., and other work was done independently to facilitate use in Japan.)

SecBoK2021(English version):https://www.jnsa.org/en/reports/secbok.html

Roles

Skills

Required knowledge and skills for each role

1	Prerequisite skills (Knowledge / skills to be possessed as a premise for job performance)
2	Required skills (Knowledge / skills required to carry out job performance)
3	Reference skills (Not required for job performance but desirable knowledge / skills)

※Relationship between"Prerequisite skills" and "Required skills"
If you secure human resources with prerequisite skills and provide education and training on required skills to the person, he/she will be able to take the job..

<Level of knowledge and skills>

L	Low(less than 3 years experience)
M	Medium (more than 3 years of experience or related exercises / training participants can cope)
H	High (10 or more years of experience or experienced professional who assumed advanced training or "prominent personnel" can cope)
P	Pending (related to information gathering and intelligence. It is not a subject to leveling this time)

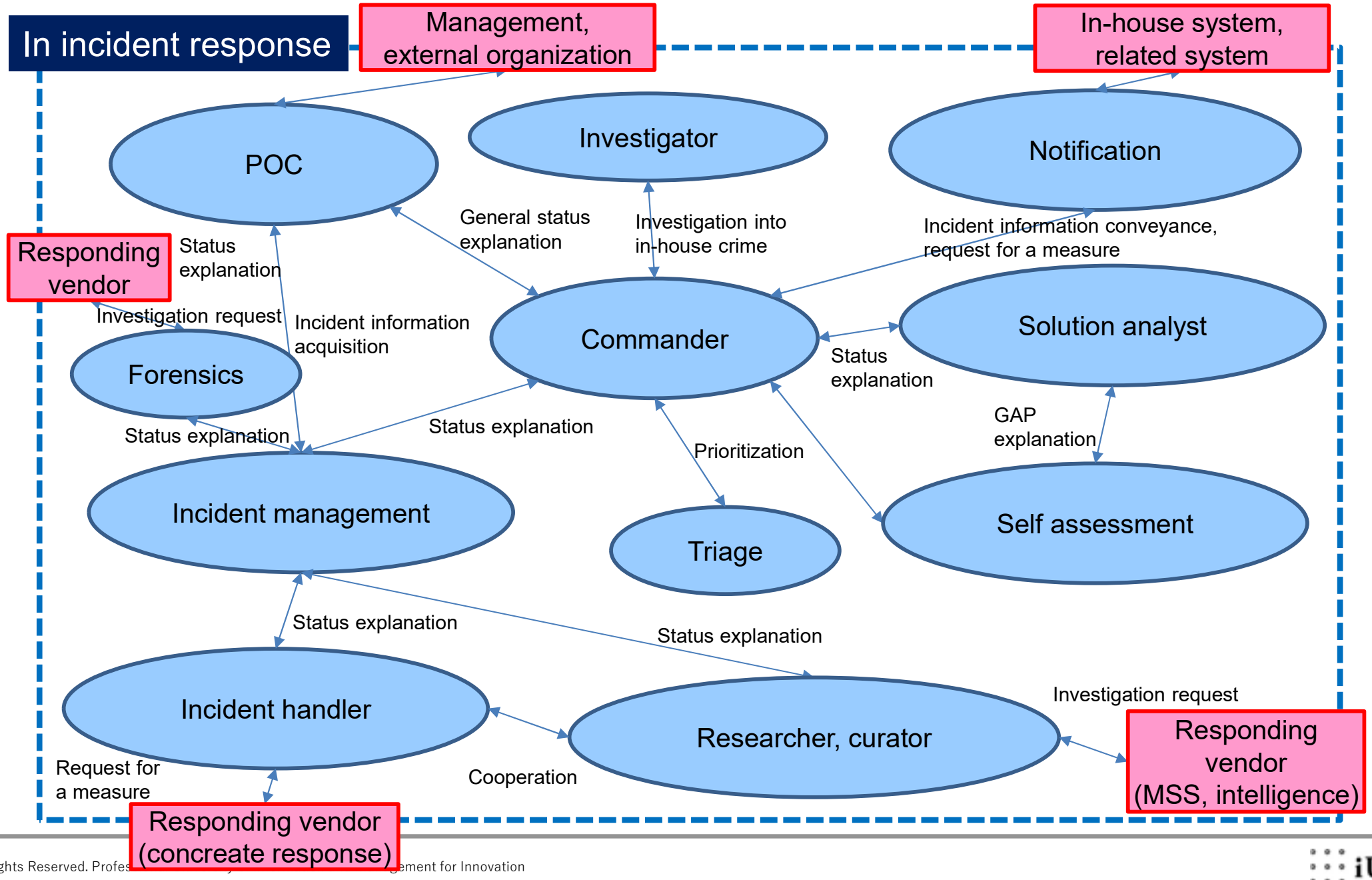
	KSA -ID	Old / New	Old NICE ID	Field	Category	Subcategory	Level	KSA (knowledge, Skill, Ability) Description	CISO	PUC	Notification	Commander,Triage	Incident manager,Incid handler	Curator	Researcher	Self assessment,Solut analyst	Vulnerability diagnos consultant	Education / Awareness raising	Forensic engineer	Investigator	Legal advisor	IT planning division	IT system division	Information security auditor
1	K0052	Similar Term exists in Old NICE	75	00 Basis	1 Mathematical and Physical Informatics		L	Knowledge of mathematics (e.g. logarithms, trigonometry, linear algebra, calculus, statistics, and operational analysis).								3								
2	K0030	Similar Term exists in Old NICE	42	00 Basis	2 Computer/Communication Engineering		L	Knowledge of electrical engineering as applied to computer architecture (e.g., circuit boards, processors, chips, and computer hardware).																
3	K0036	Same term as Old NICE	52	00 Basis	2 Computer/Communic		L	Knowledge of human-computer interaction principles.						1		1								
4	K0055	Same term as Old NICE	78	00 Basis	2 Computer/Communic		L	Knowledge of microprocessors.																
5	K0061	Almost same Term as Old NICE	92	00 Basis	2 Computer/Communication Engineering		L	Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol [TCP] and Internet Protocol [IP], Open System Interconnection Model [OSI], Information Technology Infrastructure Library, current version [ITIL]).	2		1		1		1	1	1		1				1	
6	K0108	Similar Term exists in Old NICE	261	00 Basis	2 Computer/Communication Engineering		L	Knowledge of concepts, terminology, and operations of a wide range of communications media (computer and telephone networks, satellite, fiber, wireless).						3									1	
7	K0109	Similar Term exists in Old NICE	264	00 Basis	2 Computer/Communication Engineering		L	Knowledge of physical computer components and architectures, including the functions of various components and peripherals (e.g., CPUs, Network Interface Cards, data storage).						1	1			1	1					
8	K0113	Almost same Term as Old NICE	278	00 Basis	2 Computer/Communication Engineering		L	Knowledge of different types of network communication (e.g., LAN, WAN, MAN, WLAN, WWAN).		2		1	1	1	1								1	
9	K0114	Almost same Term as Old NICE	281	00 Basis	2 Computer/Communication Engineering		L	Knowledge of electronic devices (e.g., computer systems/components, access control devices, digital cameras, digital scanners, electronic organizers, hard drives, memory cards, modems, network components, networked appliances, networked home control devices, printers, removable storage devices, telephones, copiers, facsimile machines, etc.).													3				
10	K0138	Similar Term exists in Old NICE	903	00 Basis	2 Computer/Communic		L	Knowledge of Wi-Fi.				1	1			1							1	
11	K0395	Almost same Term as Old NICE	22	00 Basis	2 Computer/Communication Engineering		L	Knowledge of computer networking fundamentals (i.e., basic computer components of a network, types of networks, etc.).						1	1		1		1					1
12	K0491	New Term	—	00 Basis	2 Computer/Communication Engineering		L	Knowledge of networking and Internet communications fundamentals (i.e. devices, device configuration, hardware, software, applications, ports/protocols, addressing, network architecture and infrastructure, routing, operating systems, etc.).					1	1	1	1	1		1			1	1	1
13	K0516	New Term	—	00 Basis	2 Computer/Communication Engineering		L	Knowledge of physical and logical network devices and infrastructure to include hubs, switches, routers, firewalls, etc.					1	1	1	1	1		1			1	1	1
14	K0555	New Term	—	00 Basis	2 Computer/Communic		L	Knowledge of TCP/IP networking protocols.					1	1	1	1	1		1			1	1	1
15	K0556	New Term	—	00 Basis	2 Computer/Communic		L	Knowledge of telecommunications fundamentals.					1	1	1	1	1		1			1	1	1
16	K0015	Same term as Old NICE	21	00 Basis	3 Software		L	Knowledge of computer algorithms.						1	1	1	1		1					
17	K0016	Similar Term exists in Old NICE	23	00 Basis	3 Software		L	Knowledge of computer programming principles						1	1	1	1		1					

All Rights Reserved. Professional University of Information and Management for Innovation

iU

Linkage of each role in CSIRT with SecBoK

Task Chart of Information Security Engineers by Nippon CSIRT Association (NCA)



All Rights Reserved. Profes gement for Innovation

Features of SecBoK 2021　NIST SP800-181 Coordination 2

	Work role	Work Role Description (Main roles in user company)		Work Role Name of NICE Definition	Work roles definition in NICE
1	CISO (Chief Information Security Officer)	Manages internal information security. From a security perspective, confront the CIO (Chief Information Security Officer) and the CFO (Chief Financial Officer) as needed.	1	Authorizing Official / Designating Representative	Senior official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.
			27	Executive Cyber Leadership	Executes decision-making authorities and establishes vision and direction for an organization's cyber and cyber-related resources and/or operations.
			31	IT Investment / Portfolio Manager	Manages a portfolio of IT investments that align with the overall needs of mission and enterprise priorities.
2	POC (Point of Contact)	Be a contact point for external organizations such as JPCERT / CC(*1), NISC(*2), police, line ministry, NCA(*3), other CSIRTs, etc. Be a contact point as an IT department coordinator for internal sections such as legal section, external affairs, IT department, public relations and other business divisions, and share information among them.		No respondending role	
3	Notification	Coordinate the organization and disseminate information to relevant departments in the company. Coordinate with the IT department when it affects internal systems.		No respondending role	
4	Commander	Perform overall control of security incidents that occur in your organization. Share information with CISO and managements when critical incidents. happended In addition, support CISO and managements for their decision making.	27	Executive Cyber Leadership	Executes decision-making authorities and establishes vision and direction for an organization's cyber and cyber-related resources and/or operations.
4	Triage	Determine priorities in response to events.	27	Executive Cyber Leadership	Executes decision-making authorities and establishes vision and direction for an organization's cyber and cyber-related resources and/or operations.
5	Incident manager	Give instructions to the incident handler to monitor the response status of the incident. Manage the response history and report the situation to the commander.	35	Cyber Defense Incident Responder	Investigates, analyzes, and responds to cyber incidents in your network environment or enclave.
5	Incident handler	Handle the incident. If the process is outsourced to a security vendor, issue an instruction to cooperate and manage. Report the status to the incident manager.	35	Cyber Defense Incident Responder	Investigates, analyzes, and responds to cyber incidents in your network environment or enclave.
6	Curator	Analyze the information collected by the researcher and select whether the information should be applied to the organization. Often used as a security operation center (SOC) in conjunction with researchers.	37	Threat/Warning Analyst	Develops cyber indicators to maintain awareness of the status of the highly dynamic operating environment. Collects, processes, analyzes, and disseminates cyber threat/warning assessments.
7	Researcher	Collects security events, threat information, vulnerability information, profile information on attackers, information on international affairs/trends, media information, etc. and provides the collected inforarmation to the Curator. It is collected only and not analyzed.	33	Cyber Defense Analyst	Uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events that occur within their environments for the purposes of mitigating threats.
8	Self assessment	Formulate a security strategy in line with the business plan of your organization. Perform risk assessment based on Fit & Gap of the current situation and Tobe image, develop a solution map and promote adoption. Confirm the effectiveness of the introduced solution and reflect it in the improvement plan.	18	Systems Security Analyst	Responsible for the analysis and development of the integration, testing, operations, and maintenance of systems security
8	Solution analyst	Perform risk assessment in normal times. When responding to incidents, respond to vulnerability analysis, impact investigation, etc.	18	Systems Security Analyst	Responsible for the analysis and development of the integration, testing, operations, and maintenance of systems security
9	Vulnerability diagnostic consultant	Check whether the network, OS, middleware, and applications are coded in a secure programming manner, and evaluate the diagnostic results.	36	Vulnerability Assessment Analyst	Performs assessments of systems and networks within the network environment or enclave and identifies where those systems/networks deviate from acceptable configurations, enclave policy, or local policy. Measures effectiveness of defense-in-depth architecture against known vulnerabilities.
10	Education / Awareness raising	Conduct education and enlightenment activities to improve and to raise bottom of IT literacy in your organization.	21	Cyber Instructional Curriculum Developer	Develops, plans, coordinates, and evaluates cyber training/education courses, methods, and techniques based on instructional needs.
			22	Cyber Instructor	Develops and conducts training or education of personnel within cyber domain.
			25	Cyber Workforce Developer and Manager	Develops cyberspace workforce plans, strategies, and guidance to support cyberspace workforce manpower, personnel, training and education requirements and to address changes to cyberspace policy, doctrine, materiel, force structure, and education and training requirements.
11	Forensic engineer	Perform systematic investigation, precision inspection, analysis and reporting. Since a malicious person may try to eradicate evidence, it is also required to restore the eradicated data and track the footprint, along with the preservation of evidence.	51	Law Enforcement/Counterintelligence Forensics Analyst	Conducts detailed investigations on computer-based crimes establishing documentary or physical evidence, to include digital media and logs associated with cyber intrusion incidents.
			52	Cyber Defense Forensics Analyst	Analyzes digital evidence and investigates computer security incidents to derive useful information in support of system/network vulnerability mitigation.
12	Investigator	Investigate external crimes and internal crimes. Security incidents differ from system failures in that malicious persons exist. As with ordinary criminal investigations, it is required to logically narrow down the investigation target while clarifying the motives, securing the evidence, and presuming the next event to occur.	50	Cyber Crime Investigator	Identifies, collects, examines, and preserves evidence using controlled and documented analytical and investigative techniques.
13	Legal advisor	Advise on the system regarding what should be observed from compliance and legal point of view	19	Cyber Legal Advisor	Provides legal advice and recommendations on relevant topics related to cyber law.
14	IT planning division	Make plans for internal IT use. Conduct research and analysis of IT usage as needed.	26	Cyber Policy and Strategy Planner	Develops and maintains cybersecurity plans, strategy, and policy to support and align with organizational cybersecurity initiatives and regulatory compliance.
			29	IT Project Manager	Directly manages information technology projects.
15	IT system division	Promote internal IT projects, as well as design, development, operation and maintenance of application systems.	16	Network Operation Specialist	Plans, implements, and operates network services/systems, to include hardware and virtual environments.
			17	System Administrator	Responsible for setting up and maintaining a system or specific components of a system (e.g. for example, installing, configuring, and updating hardware and software; establishing and managing user accounts; overseeing or conducting backup and recovery tasks; implementing operational and technical security controls; and adhering to organizational security policies and procedures).
			23	Information Systems Security Manager	Responsible for the cybersecurity of a program, organization, system, or enclave.
			24	Communications Security (COMSEC) Manager	Individual who manages the Communications Security (COMSEC) resources of an organization (CNSSI 4009) or key custodian for a Crypto Key Management System (CKMS).
			34	Cyber Defense Infrastructure Support Specialist	Tests, implements, deploys, maintains, and administers the infrastructure hardware and software.
16	Information security auditor	In order to effectively carry out information security risk management, verify or evaluate the status of preparation and operation of appropriate control measures based on risk assessment according to the standards, and then provide assurance or advice.	32	IT Program Auditor	Conducts evaluations of an IT program or its individual components to determine compliance with published standards.

Among the 52 roles in NIST SP800-181, associated roles were picked out and coordinated with the 16 roles in SecBoK 2021.

All Rights Reserved. Professional University of Information and Management for Innovation

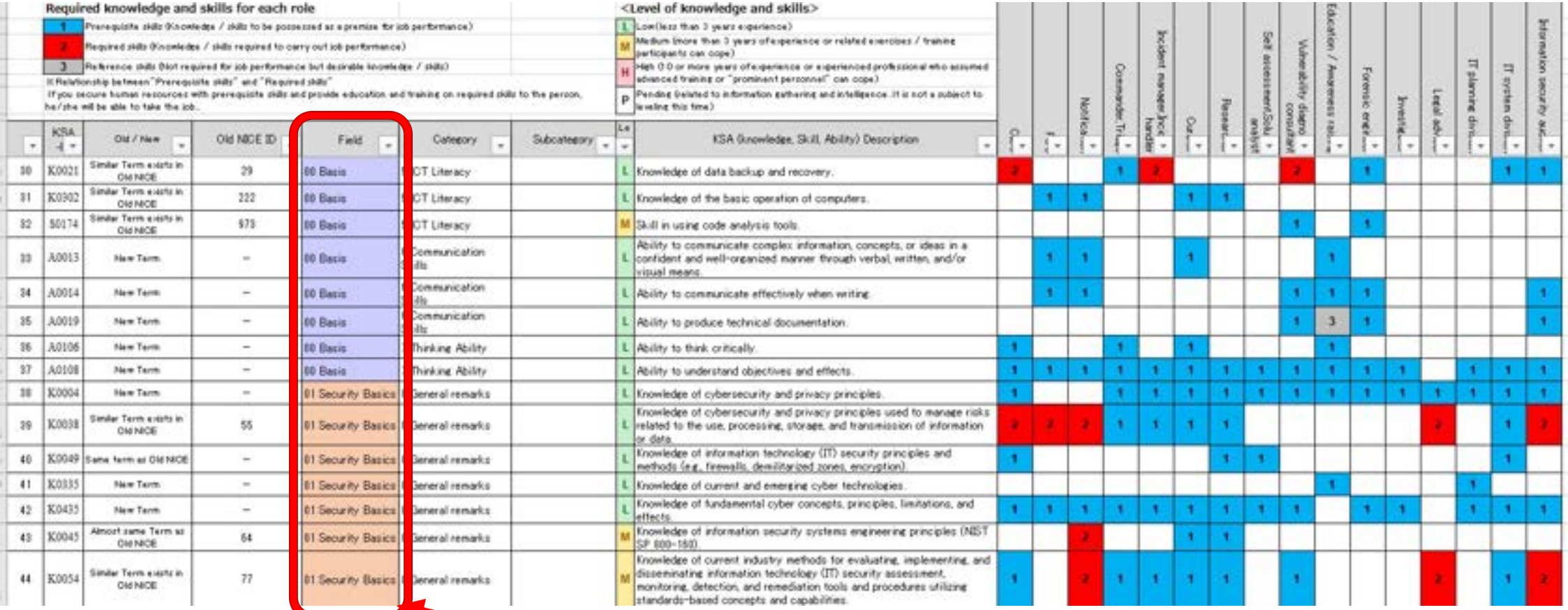
5. Skills required for plus security human resources

-Utilizing SecBoK-

All Rights Reserved. Professional University of Information and Management for Innovation

Examples of SecBoK's use in developing plus security human resources.

A unique feature of SecBoK is that it incorporates security literacy and security basics skill items.
These skill items are necessary for "Plus security human resources".



All Rights Reserved. Professional University of Information and Management for Innovation

Case Example of Educational Application (Information Technology University)
Computer Science Curriculum Standard (J17)

The Computing Curriculum Standard J07 is a compilation of the computer science (CS), information system (IS), computer engineering (CE), software engineering (SE), information technology (IT) and general information processing education (GE) domains. The curriculum standard follows a review of the status of specialized information technology education in Japan. After it was reviewed in 2017, J17 was published.

Field | Major Item | Middle Item	CS	IS	CE	SE	IT	GE	CyS ICT Basics	CyS Security Basics	CyS Security Specialization
Basics | ICT basics | Information theory	●					●	●		
Basics | ICT basics | Computer hardware	●						●		
Basics | ICT basics | Network infrastructures	●					●	●		
Basics | ICT basics | Communication protocols and services	●					●	●		
Basics | ICT basics | Data structures	●						●		
Basics | ICT basics | Databases	●					●	●		
Basics | ICT basics | Knowledge management	●					●	●		
Basics | ICT basics | Algorithms and programming	●					●	●		
Basics | ICT basics | Operating system	●					●	●		
Basics | ICT basics | Software	●					●	●		
Basics | ICT basics | System development	●					●	●		
Basics | ICT basics | System operation	▲					●	●		

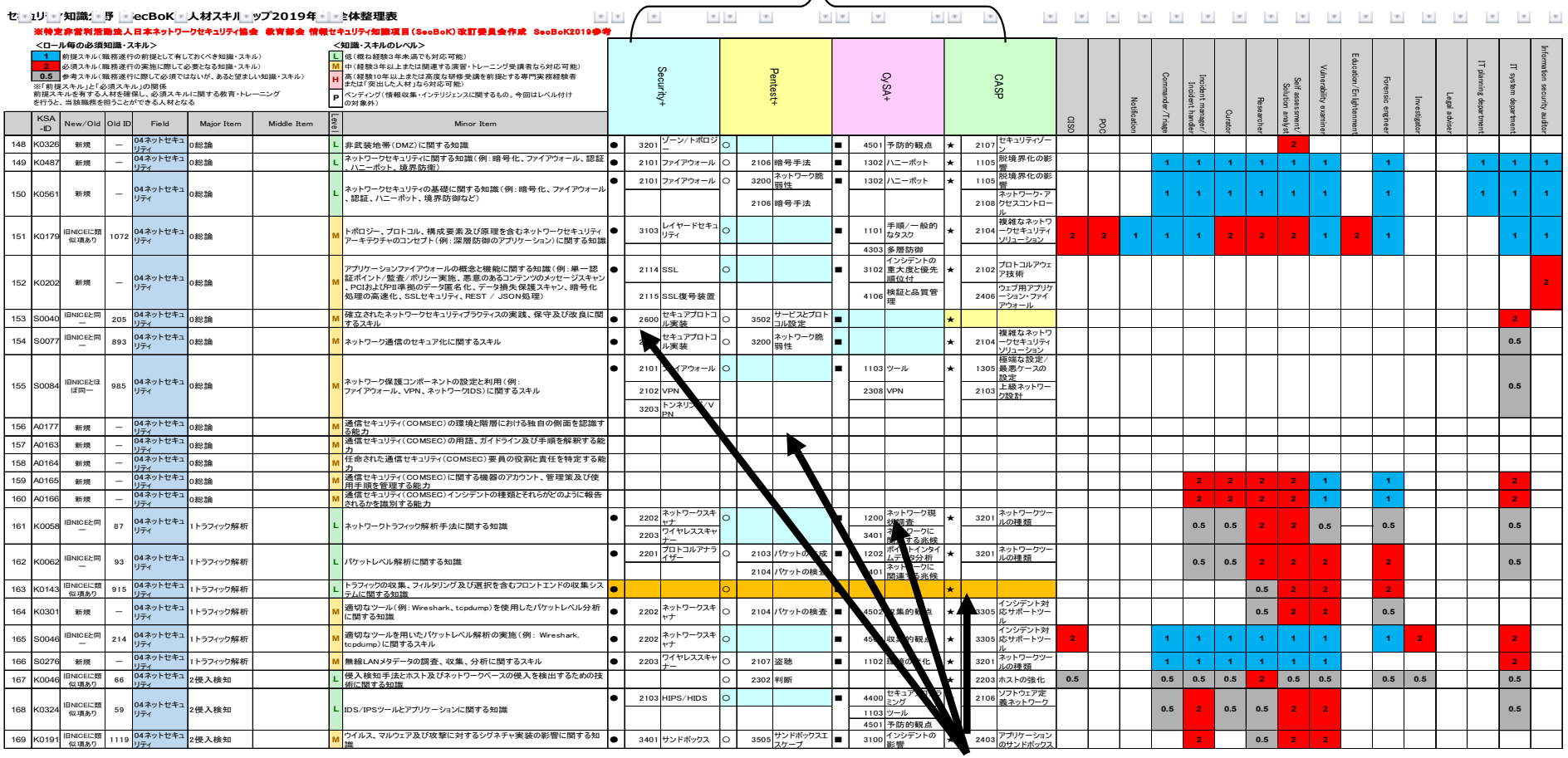
The Security Body of Knowledge (SecBoK) Human Resource Skill Map serves as a reference for the skills required of human resources. To organize the knowledge items required for the curriculum model, each specialization level in a range covering a specialized information education item in the SecBoK Human Resource Skill Map was organized as a reference for creating a cybersecurity curriculum.

All Rights Reserved. Professional University of Information and Management for Innovation

Case Example of Coordination With Qualifications
CompTIA Security-related Qualifications and SecBoK Skills

CompTIA is a vendor-neutral IT certification organization mapping the skills necessary for each qualification to SecBoK skills. This makes it possible to visualize, for example, which security roles a qualification holder would be highly suitable for. The mapping is useful not only for personal development plans but also for creating departmental and organizational structures, developing departments as a whole, and more.

Individual qualifications



Range of questions for each qualification, and prerequisite skills

All Rights Reserved. Professional University of Information and Management for Innovation

Next stage of required security human resource

1. Would a lack of security human resources change?

   Required human resources are **changing**

2. Is security not a matter of the non-security department?

   Security is essential for **the companies survive in the tide of DX**

3. What kind of security human resources are required for business departments as system users?

   Not for defense, **“proactive security” to make benefits** has emerged. Make user/business departments be aware of security too.

4. Critical “proactive plus security human resources” for the future of companies in Japan

   There is no way to go without “DX” for Japanese companies to survive in the future. For the success of DX, **develop** “**proactive** plus security human resources” that is **severely deficient**.

SecBoK is unique in that it can be used not only for traditional "security professional" development, but also for "plus security human resources" development, and can be used by many people!

All Rights Reserved. Professional University of Information and Management for Innovation

Professional University of Information and Management for Innovation (i-University)

All Rights Reserved. Professional University of Information and Management for Innovation