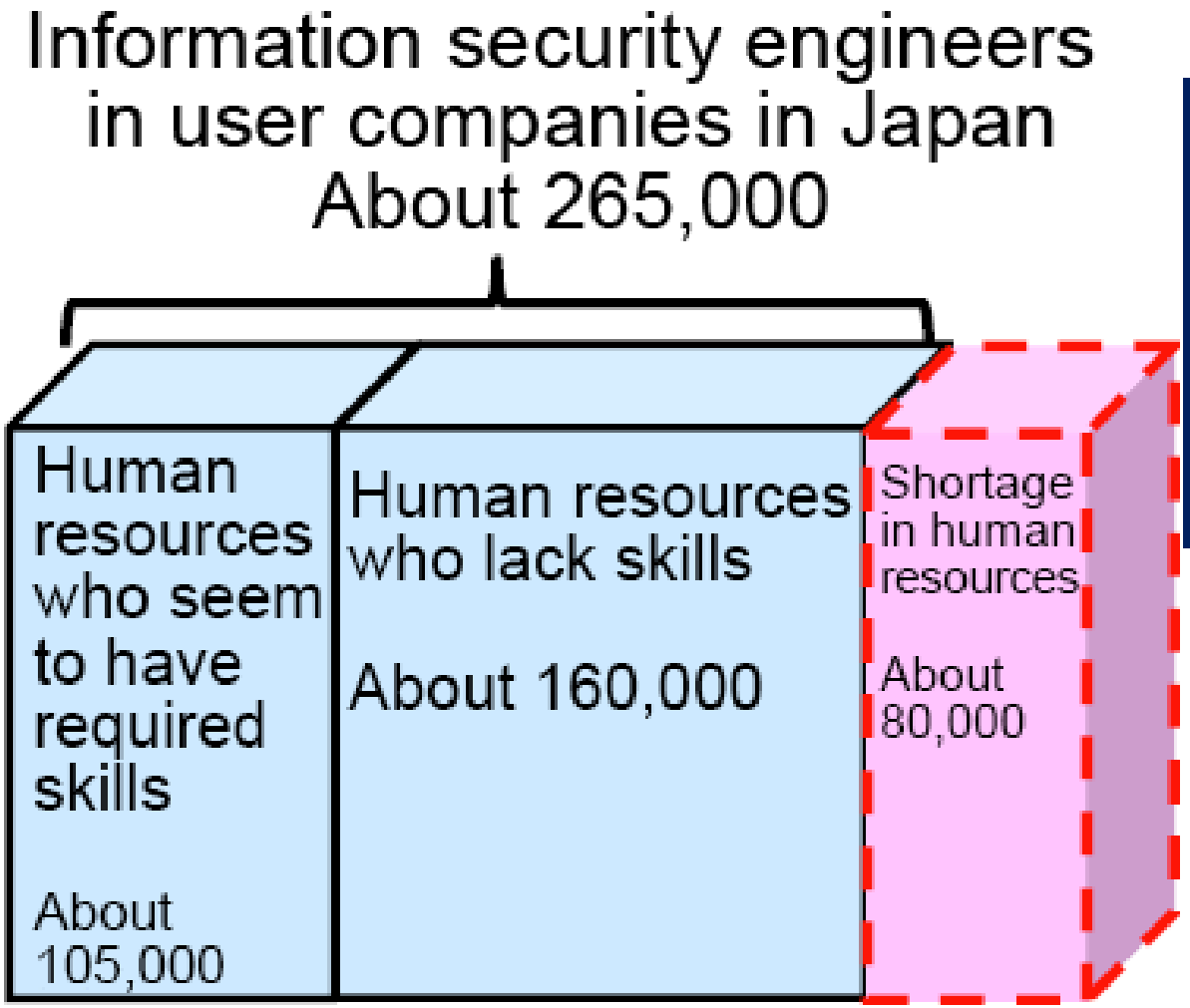
SecBoK 2019 - Background and How to Use It for Developing Security Human Resources

Toshihiro Hirayama, Chairperson,
Education Committee, Japan Network Security Association

1. Need More Information Security Engineers

What types of engineers?
How do we increase them?

What Types of Engineers? What is Needed?



According to a research by IPA, user companies in Japan need much more information security engineers (about 80,000 people needed).

<Estimated by IPA based on additional analysis on human resource shortage conducted to supplement the "Basic Survey on Information Security Human Resource Development" (basic survey in 2012 and additional analysis in 2014)>

Which Industries (Business Types) Need Much More Engineers?

	Industry	(Strength)
1	Agriculture, forestry, fishery, and mining	256
2	Construction, civil engineering, and related industries	2,764
3	Electronic component, device, and electronic circuit manufacturing	1,403
4	Information and communication equipment and apparatus manufacturing	605
5	Electric machinery and apparatus manufacturing	1,150
6	Other manufacturing industries	15,853
7	Electricity, gas, heat supply, and water	81
8	Communication	683
9	Information services	1,885
10	Other information and communication industries	1,717
11	Transportation and postal	6,716
12	Wholesale and retail	14,480
13	Finance and insurance	4,957
14	Real estate and goods rental and leasing	1,547
15	Scientific research and professional engineers	1,014
16	Accommodations and eating and drinking services	3,535
17	Living-related services and amusement services	3,301
18	Education and learning support	2,094
19	Medical and welfare	8,473
20	Compound services	614
21	Other service industries	8,462
	Total	81,590

Especially, user businesses such as the following are outstanding, other than IT businesses:

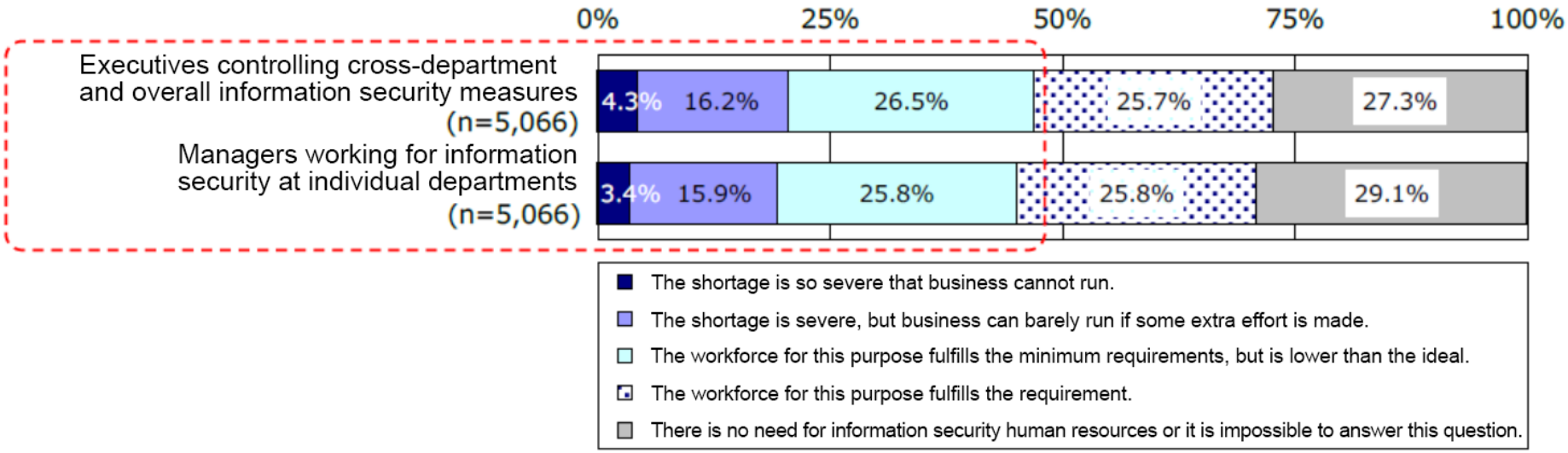
- Manufacturing
- Wholesales/Retail
- Medial/Welfare

Source
http://www.meti.go.jp/committee/sankoushin/shojo/johokeizai/it_jinzai_wg/pdf/002_03_00.pdf

Current Status of Security Engineer Shortage in User Companies

About 3 to 4% of the responsible persons in user companies said, "We need security engineers. We are now in a critical state in which we cannot continue our business."

Shortage in human resources handling in-house information security measures

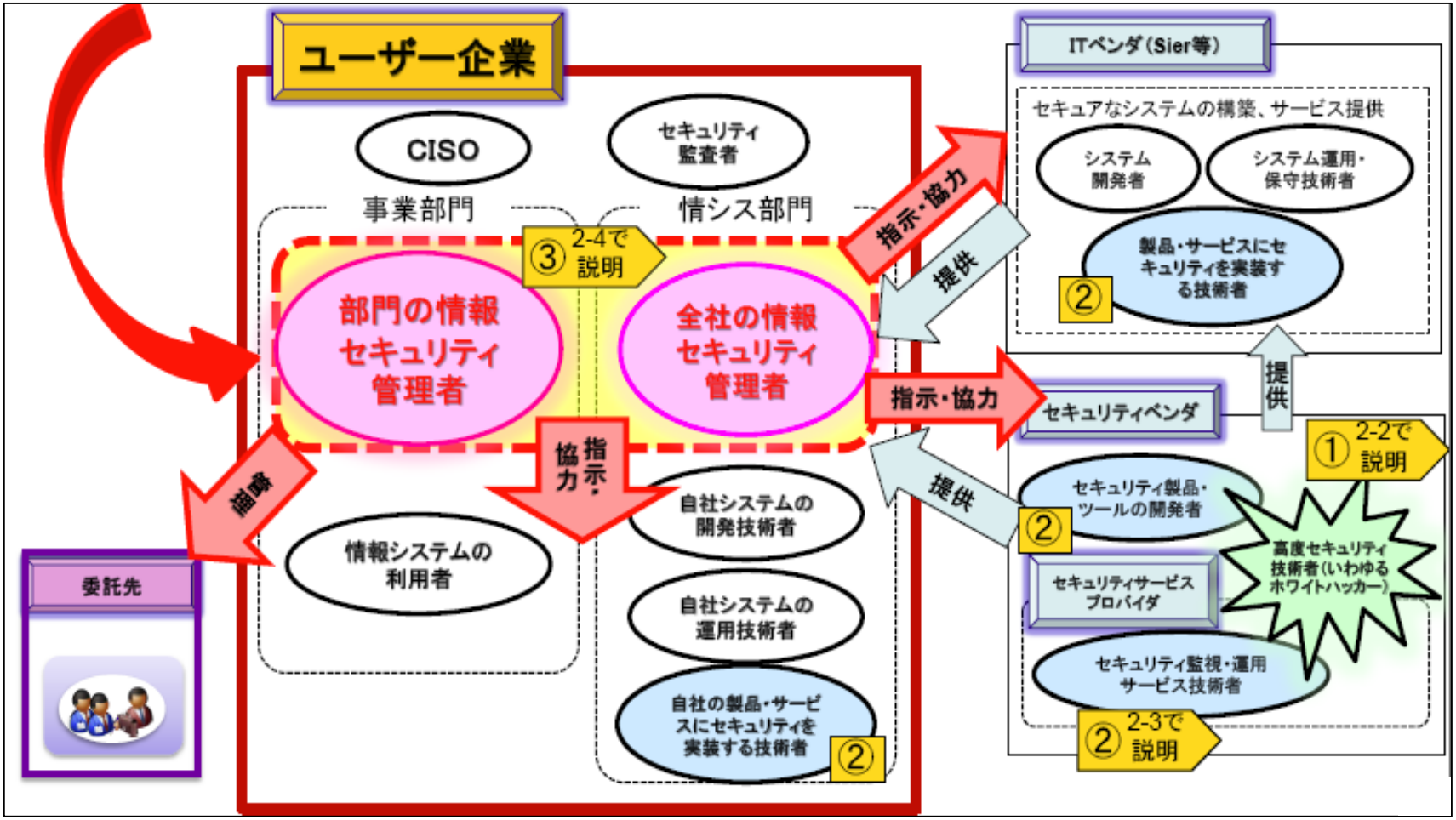


("Web Questionnaire Survey on Human Resources Engaged Handling In-house Information Security Measures" conducted in December 2015)

Reference: *Results of Research on Latest Trend and Future Estimate of IT Human Resources*, Ministry or Economy, Trade and Industry
http://www.meti.go.jp/press/2016/06/20160610002/20160610002-7.pdf

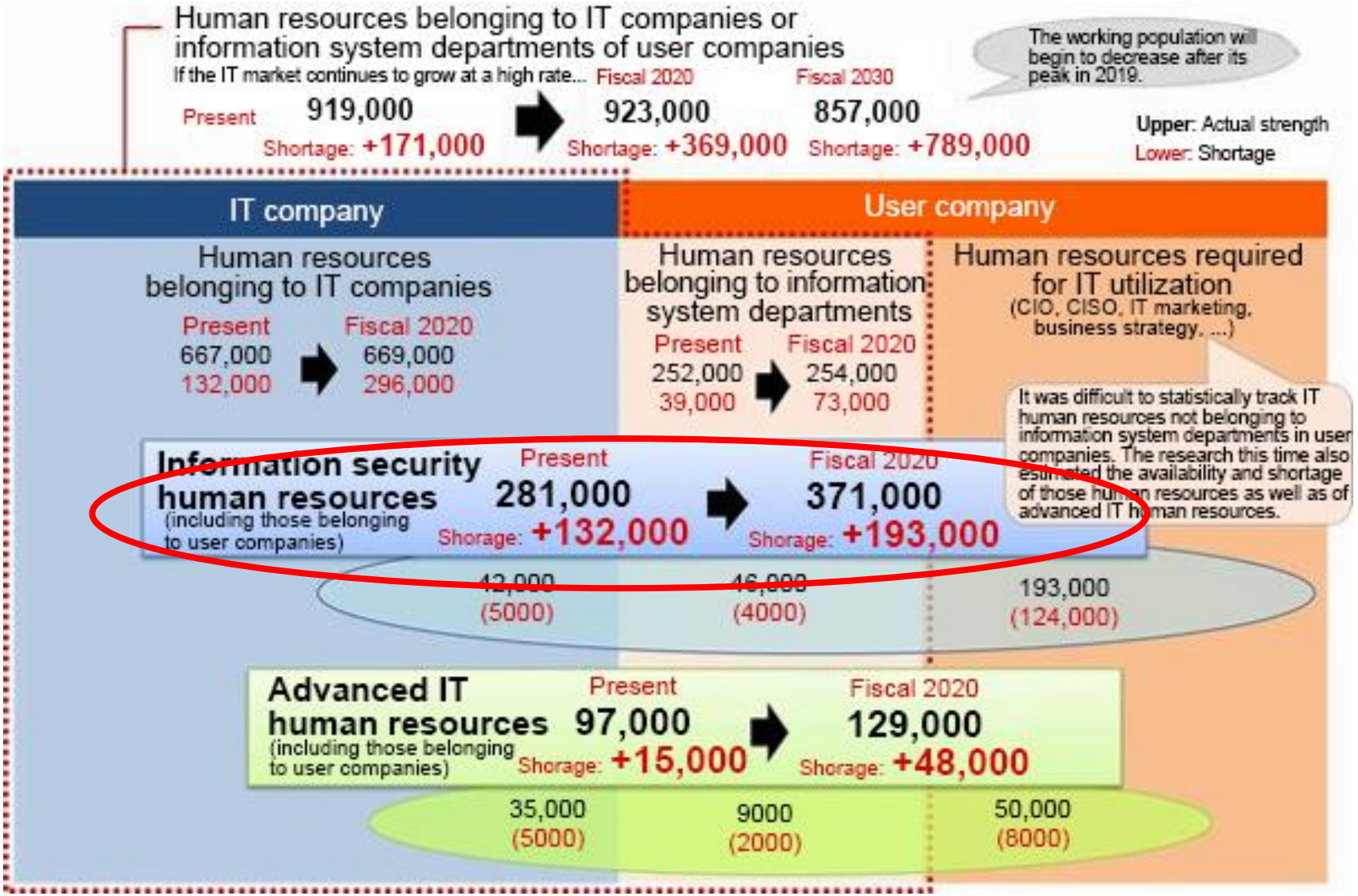
What Types of Security Engineers Will Be Needed?

(1) High-level security engineer like a white hacker
(2) Persons with the security technologies to build a secure information system
(3) Persons managing the information security in a user company in cooperation with in-house security engineers



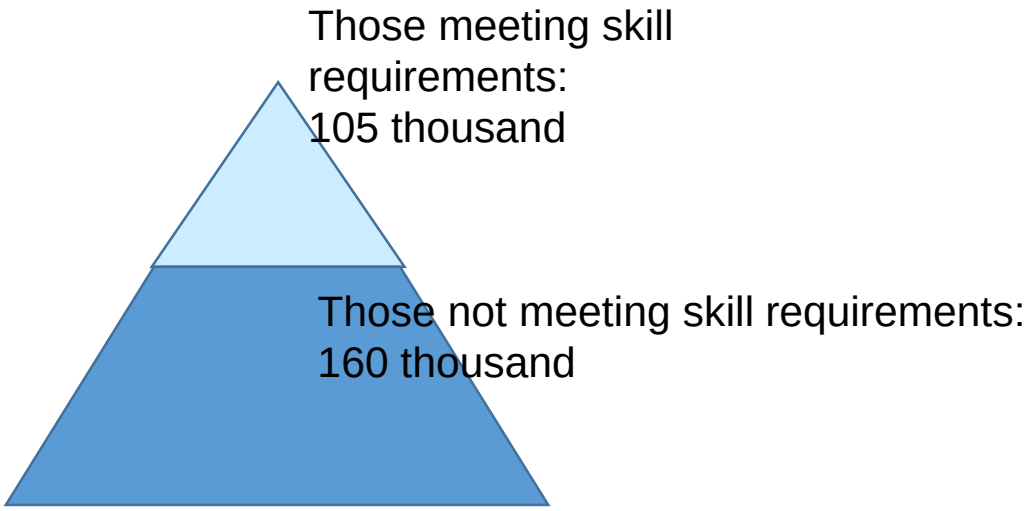
Excerpt from the *Needs for Human Resources in the Information Security Field*, Information Processing Promotion Section, Ministry of Economy, Trade and Industry, March of 2015

Security workforce shortage tends to become more severe. That is also accelerated by the working population reduction.

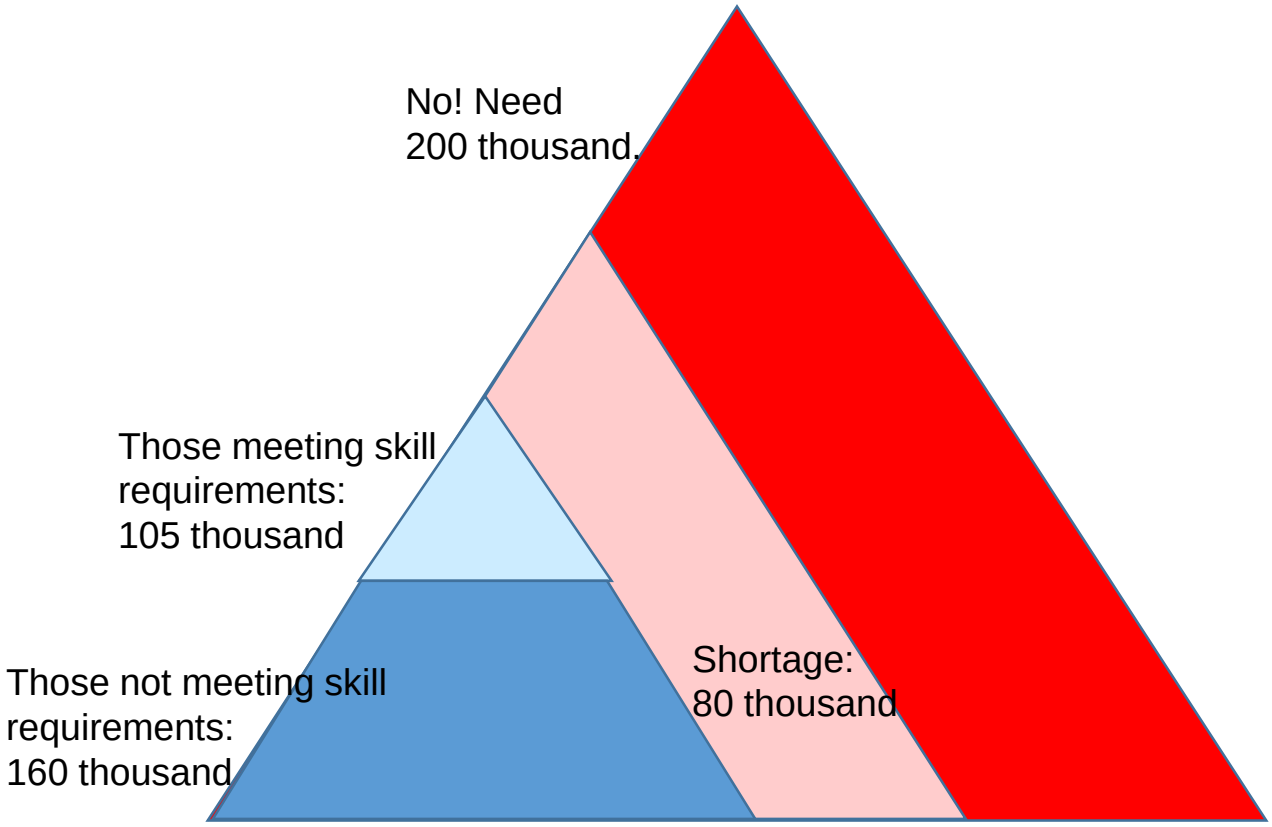


Source: http://www.meti.go.jp/press/2016/06/20160610002/20160610002.html

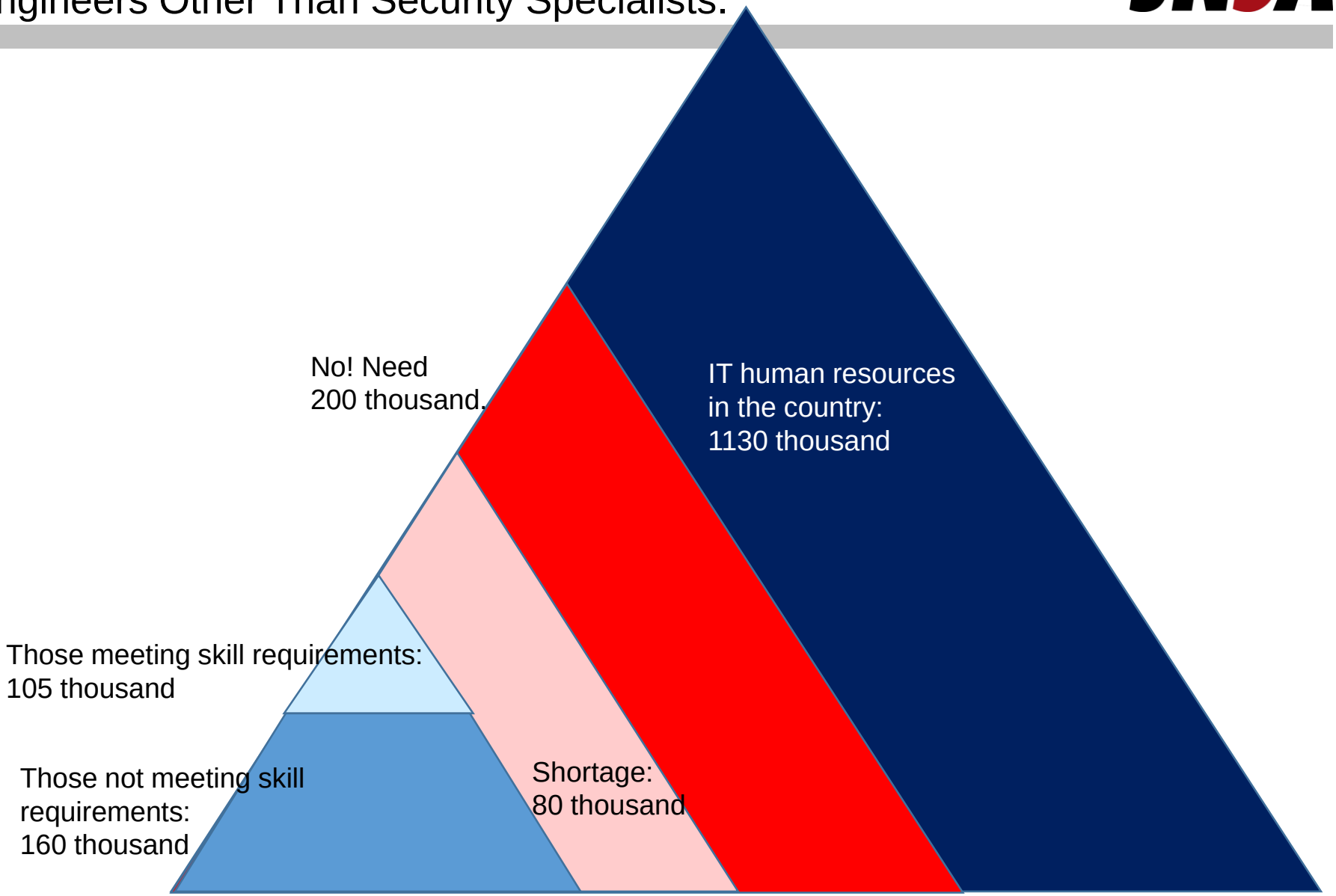
Number of Security Engineers in Japan



We Still Need Much More Engineers.



The Number of Engineers Does Not Increase. We Count on Engineers Other Than Security Specialists.



Long-Awaited?
Guidance for Developing Security Engineers

YAHOO! JAPAN ニュース

IDでもっと便利に新規取得
ログイン　熊本地震災害の緊急支援募金を受付中

キーワードを入力　ニュース

トップ | 速報 | 写真 | 映像 | 雑誌 | 個人 | ビジネス | 特集

ビジネストップ | 経済 | 企業 | グローバル | マーケット | キャリア | テクノロジー

我が社に必要なセキュリティ人材が分かる資料、JNSAが7年ぶり改訂

ITmedia エンタープライズ 4月20日(水)17時21分配信

ユーザー系企業で求められる人材の役割（JNSA資料より）

日本ネットワークセキュリティ協会（JNSA）の教育部会は4月19日、「セキュリティ知識分野（SecBoK）人材スキルマップ2016年版」を公開した。2009年以来の改訂では情報セキュリティ人材の16の役割と役割ごとに必要な知識について体系的に取りまとめている。

【その他の画像】

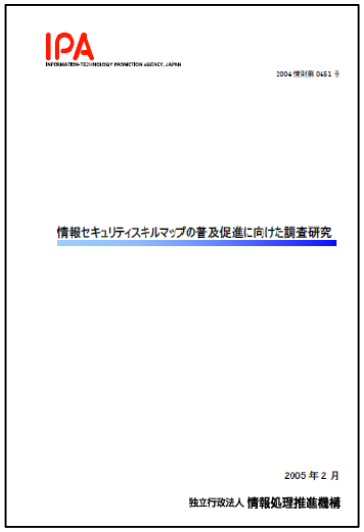
2. What Should We Learn?

Information Security Body of Knowledge, SecBoK (Security Body of Knowledge)

Development of Information Security Engineers (1)

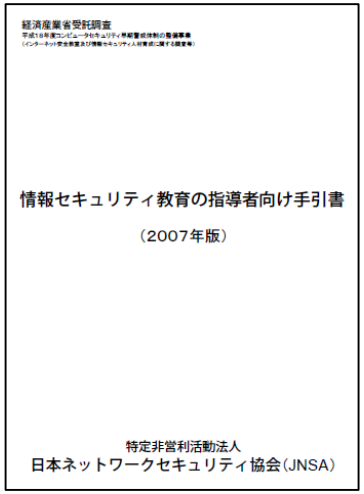
1) Requested from IPA, the Information Security Skill Map was created in 2004 and 2005 (revision).

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, 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



Development of Information Security Engineers (2)

3) ISEPA released the *Guidebook of Human Resource Architecture for Information Security*.

ISEPA (Information Security Education Providers Association) released a guide for human resource development in 2009.
http://www.jnsa.org/isepa/images/outputs/jinzai_arch_2009.pdf

4) Using SecBoK as a reference, we published the *Textbook for Information Security Professionals* in 2009.

http://ascii.asciimw.jp/books/books/detail/978-4-04-867782-0.shtml

SecBoK (Before Revision): Job Classification

Human Resource Development Map by Job Types of the
Information Security Human Resource Architecture

JNSA

	職種	定義
1	プリセールスエンジニア	セキュリティ製品導入を検討する企業に対し、どのような環境なら顧客の要望が実現可能なのか製品・サービスに関する技術的知識を持って営業活動を支援する
2	セールスコンサルタント	顧客システムの現状の把握および問題点の調査し、顧客の状況に合わせて、適用範囲が広範囲な製品・ソリューション対策/提案をする
3	テクニカルコンサルタント	情報セキュリティに関する経験値が高く、技術的見地からのアドバイスやレビューを行う
4	セキュリティアーキテクト(製品・ソリューション)	セキュリティ製品・ソリューション開発の設計、及び管理
5	セキュリティアーキテクト(コンサル)	セキュリティ確保、情報漏洩防止等におけるコンサルティング・設計・実装および支援業務
6	セキュリティエンジニア(要求定義)	セキュリティ・ソリューションに関する要求定義を行う
7	セキュリティエンジニア(企画・設計)	セキュリティ・ソリューションの企画・設計・最新技術調査、製品評価
8	セキュリティエンジニア(基盤)	セキュリティ・システムの基盤部分(OS・ネットワーク)の全体設計・運用設計・方式設計、開発
9	セキュリティエンジニア(アプリ)	アプリケーションの開発フェーズにおいてセキュリティの確保を行う
10	セキュリティエンジニア(DB)	DBMSを構成要素とするシステムを対象に、セキュリティの確保を行う
11	QAマネージャー	品質保証業務及びそのプロセス改善業務。製品品質に関する顧客窓口業務。開発チームに対する品質保証啓蒙活動
12	QAエンジニア	ソフトウェア開発および開発プロジェクトに対し、品質保証全般のテストを実施。
13	セキュリティテスター	ソースコード解析や脆弱性の洗い出し
14	プログラマー	仕様書や設計書に従って、セキュアプログラミングの知識を持ってプログラムを作る。
15	プロジェクトマネージャー	プロジェクトの計画と実行に於いて総合的な責任を持つ。期日までに成果物を完成させる。
16	セキュリティシステムアドミニストレーター	システムに対するセキュリティ対策を整備し、運用管理を行う
17	オペレーター	提供しているサービスの運用・監視を行う。 ネットワーク監視。ヘルプデスク。サービスシステム維持管理等
18	セキュリティアナリスト	各種ログを分析し、インシデントを抽出し、予兆を発見し、対策を提示
19	フォレンジックアナリスト	証拠証跡の分析を行い、証拠保全、証拠開示手続きも行う
20	インシデントハンドラー(プロダクト)	プロダクトに確認された脆弱性の分析と関係部署との調整をおこなう
21	インシデントハンドラー(組織)	攻撃発生時のインシデント分析及び対処と関係部署との調整をおこなう
22	フィールドエンジニア	顧客現場で、セキュリティシステム構築に伴う、システム機器の設置から設定保守・修理を行う
23	プライバシーオフィサー	企業・団体内の個人情報保護体制の構築、運用、改善を行う
24	プライバシースペシャリスト	企業の個人情報保護に関して、規定作成から意識向上施策実施までを担当する
25	CSO/CISO/CIAO	情報資産保護を経営の観点から意思決定をし、指揮をとり、組織の情報資産保護の責任をとる
26	CSO/CISO/CIAO補佐	CSO/CISO/CIAOの業務を補佐し、経営陣の意思を現場に浸透させ、施策がきちんと実行されるかを監視する
27	セキュリティプロダクトオーナー	セキュリティ製品の企画から保守にいたるまで製品に関わる全責任をとる
28	セキュリティサービスオーナー	セキュリティサービスの企画から保守にいたるまでサービスに関わる全責任をとる
29	セキュリティコンサルタント(マネージメント)	情報セキュリティ戦略立案から、情報資産の管理・運用方法の策定までに関し、顧客の問題解決を支援する。
30	セキュリティアドバイザー	情報セキュリティ全般に関してのアドバイスを行う
31	セキュリティストラテジスト	企業の経営戦略実現に向けて、セキュリティを活用した基本戦略を策定、提案、推進する
32	セキュリティ監査人	情報セキュリティ監査制度に対する知識と経験を有するとともに、実証された能力として、監査計画を立案し、監査計画に基づいて監査を実施し、報告書を作成し、監査結果を被監査主体に報告する

SecBoK (Before Revision): Major Categories of the Skill Map

No.	Large Category	
1	Information security management	
2	Network infrastructure security	
3	Application security	Web
		Email
		DNS (Domain Name System)
4	OS security	Unix
		Windows
		Secure OS
5	Firewall	
6	Intrusion detection	
7	Virus	
8	Secure programming techniques	
9	Security operation	
10	Content security	
11	Authentication	
12	PKI (Public Key Infrastructure)	
13	Cryptography	
14	Electronic signature	
15	Unauthorized access methods	
16	Laws and regulations and standards	

About 600 minor skill items under the middle items

IPA Released "iCD2015" in June, 2015.

Reference: http://www.ipa.go.jp/jinzai/hrd/i_competency_dictionary/icd.html

As global competition becomes severe, new IT services and IT infrastructures such as the cloud, mobile computing, and SNS have been common in late years, and business environments are changing each and every second. Therefore, to develop IT human resources that can respond to these environment changes, IPA has provided the frameworks for human resource development and promoted to use them. In this way, IPA has supported human resource development in the industries.

IPA provides "i Competency Dictionary (iCD)." This systematizes jobs of the business that utilizes IT in companies (tasks) and capability and potential of IT human resources (skill), as a "task dictionary" and "skill dictionary," respectively. Companies can use the iCD for human resource development according to the purpose based on the management strategy, etc.

IPA released a trial version of the iCD in July 31, 2014. It released the formal version, "i Competency Dictionary 2015 (hereinafter, iCD2015)," based on public comment, demonstration experiments in the industries.

The iCD2015 includes the revision of the groups of knowledge, etc. in the trial version. Besides, tasks and skills corresponding to human development necessary for the new age such as **"information security"** and "IT for business creation" were added to the iCD2015.

Skill Dictionary (Security Knowledge)

In addition to the knowledge items of the skill standard and Japan Information-Technology Engineers Examination, the *Computing Curriculum Standard* and main bodies of knowledge are used as reference. Addition of SecBoK

Skill dictionary

- **Methodology**
- **Technology**
- **Related knowledge**

11000 knowledge items were identified and sorted in original groups:

3 categories,
78 classes,
423 skill items, and
8234 knowledge items

Name	Issuing Organization
Scope of the examination of the morning part of the Japan Information-Technology Engineers Examination (body of knowledge)	Information-Technology Promotion Agency (IPA)
Common Career Skill Framework (First Edition/Supplement Edition) (CCSF) Knowledge System	Information-Technology Promotion Agency (IPA)
IT Skill Standard (ITSS) V3 2011	Information-Technology Promotion Agency (IPA)
IT Specialist Nurturing Handbook FY2008 Revision	Information-Technology Promotion Agency (IPA)
Users' Information Systems Skill Standards (UISS) Ver. 2.2	Information-Technology Promotion Agency (IPA)
Embedded Technology Skill Standards (ETSS) 2008	Information-Technology Promotion Agency (IPA)
Computing Curriculum Standard (J07)	Information Processing Society of Japan
A Guide to the Business Analysis Body of Knowledge (BABOK) Edition 1.2	International Institute of Business Analysis (IIBA)
Requirements Engineering Body Of Knowledge (REBOK) First Edition	Japan Information Technology Services Industry Association (JISA)
Strategy and Analysis Body Of Knowledge (SABOK)	Japan IT Strategist Association
Guide to the Software Engineering Body of Knowledge (SWEBOK) 2004	IEEE/ACM
A Guide to the Project Management Body of Knowledge (PMBOK) Fourth Edition	Project Management Institute (PMI)
ITIL (Information Technology Infrastructure Library) V3	itSMF Japan
Guide to the Software Quality Body of Knowledge (SQuBOK) Ver. 1.0	Union of Japan Scientists and Engineers
Guide to the Data Management Body of Knowledge (DMBOK) First Edition	DAMA International
(ISC)^2 Official CISSP CBK	(ISC)^2 Japan
Information Security Body of Knowledge (SecBoK)	**JNSA**

SecBoK2016 Revising Activity

1) Revision and update of SecBoK

Created in 2004, the current SecBoK is the contents as of year 2009 after several updates. However, it was not updated since then.
We revised it in 2015, considering that the SecBoK was required an update so that it could respond to the shortage of information security human resources in user companies today, as well as the needs in the cloud age.

2) Activity for popularizing SecBoK and promoting its use for other associations and organizations

One of the reasons why SecBoK was not updated since 2009 was because SecBoK was not used outside of the information security industry. So, at the creation of i Competency Dictionary, we examined the SecBoK were used not only in the information security industry but also in other associations and organizations.

3. Security Body of Knowledge (SecBoK) in 2016 and 2017

Direction of Revising SecBoK2016

Class	Remarks of SecBoK Revision Committee and Policy
Job Type	- 32 job types of ISEPA are too many. => How about focusing on the security system, and then organizing the types by focusing on what types business/players are there? In this way, the number of types will be reduced. => According to the business model and contents of business, it is good to organize the types by describing each type like "this field requires a person with the job type."
Knowledge Item Class	- The current skill map is too biased toward the vendor. => New concepts (cloud, virtualization, grid, SDN, etc.) must be incorporated. => Not classifying the items by users or by vendors, but based on the job types or tasks, the items can be organized regardless of companies.
Consideration	- Companies do not accept too detailed considerations. => In order that the mission and vision of an organization can be incorporated into organization models. => Distinction between normal cases and incident cases => As to whether the company handles an issue or outsources it, both responses must be made possible.
How to Proceed with	- Clarifying the job types and profiles in which much more engineers are needed, such as "personnel who can have a dialog with vendors," we will discuss the deliverables useful for the development of such human resources.

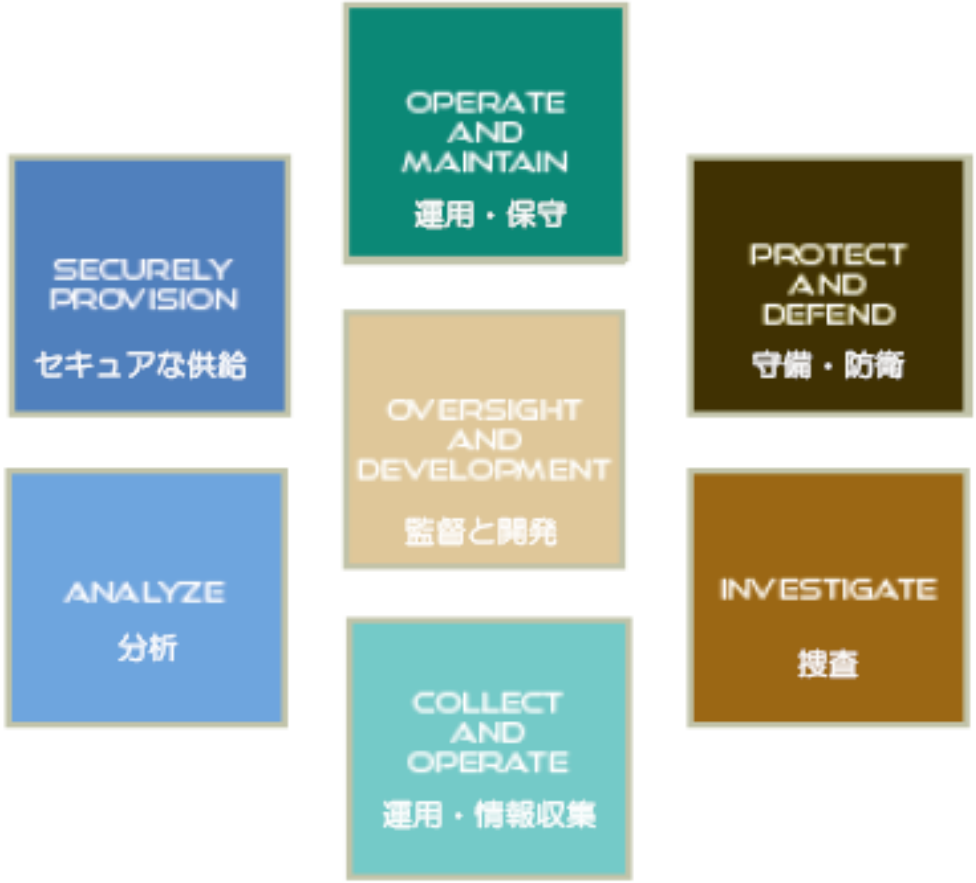
Other Frameworks

NICE: National Initiative for Cybersecurity Education

http://csrc.nist.gov/nice/

They assume that, in the United States, each ministries will create a human resource development plan based on the NICE Framework established by NIST (National Institute of Standards and Technology).

The framework organizes the cyber security field into the seven major categories.



CYBERSECURITY WORKFORCE FRAMEWORK

Categories of the NICE Framework of the United States

The NICE Cybersecurity Workforce Framework organizes the tasks and knowledge regarding the cyber security into the following seven categories.

	カテゴリ	カテゴリの定義	専門領域の例
I	セキュアな供給 Security Provision	システム開発の各過程に関わる、セキュアなIT システムの概念化、設計及び構築についての専門領域	システム要件検討、システム開発、ソフトウェア保証とセキュリティエンジニアリング、システムセキュリティアーキテクチャ、試験と評価、技術研究開発、情報保証コンプライアンス
II	運用・保守 Operate and Maintain	効果的かつ効率的なIT システムの性能とセキュリティを確保するために必 要なサポート、アドミニストレーション及び保守に関する専門領域	システム・アドミニストレーション、ネットワークサービス、システムセキュリティ分析、カスタマーサービスと技術サポート、データ・アドミニストレーション、ナレッジマネジメント
III	守備・防衛 Protect and defend	内部のIT システムやネットワークへの脅威の識別、分析及び緩和に関する専門領域	脆弱性アセスメントと管理、インシデントレスポンス、計算機ネットワーク防御（CND）分析、計算機ネットワーク防御（CND）インフラ支援
IV	捜査 Investigate	IT システム、ネットワーク及びデジタルエビデンスに関するサイバー事象及び/または犯罪についての専門領域	捜査、デジタル・フォレンジック
V	運用・情報収集 Collect and Operate	情報活動に用いられるサイバーセキュリティ情報の情報の高度な収集に関する専門領域	情報収集オペレーション、サイバーオペレーション計画、サイバーオペレーション
VI	分析 Analyze	入手したサイバーセキュリティ情報が情報活動に有効かどうかを決定するための、高度なレビューと評価に関する専門領域	脅威分析、エクスプロイト分析、ターゲット、全情報源のインテリジェンス
VII	監督と開発 Oversight and Development	他者がサイバーセキュリティ活動を効率的に実施できるようなサポートに関する専門領域	法的助言と弁護、教育と訓練、戦略策定とポリシー開発、情報システムセキュリティオペレーション（ISSO）、最高情報セキュリティ責任（CISO）

Types and Roles of Security Specialists

Malware analyst

Analyzes malware that intruded and a used exploit in a safe way to clarify the attack method and devise countermeasures. In addition, he/she can also detect unknown malware from traces left in the system/network.

Forensic analyst

Detects evidences in the system/network in cased of an incident, and preserves them appropriately.

Penetration tester

Is familiar with the latest attach methods, and proposes countermeasures. He/she can plan an examination to check for vulnerability in the system/network and conduct it appropriately, as needed.

Incident handler

Can quickly responds to the incident in case of an incident, and takes measures in cooperation with the operator and administrator of the system/network for safe recovery.

Network analyst

Operates and manages the system/network. He/she can also take the initial response in case of an incident.

Professional sales

Has basic knowledge/skill for considering and proposing security measures that are necessary for an organization, and can also propose an optimum solution from the viewpoint of business strategy.

Types and Roles of People Who Build an IT System

Consultant

Understands customers' needs and offers proposals. He/she takes responsibility for customer satisfaction.

Project manager

Understands business requirements and IT requirements, and defines requirements. He/she takes responsibility for the project.

IT specialist

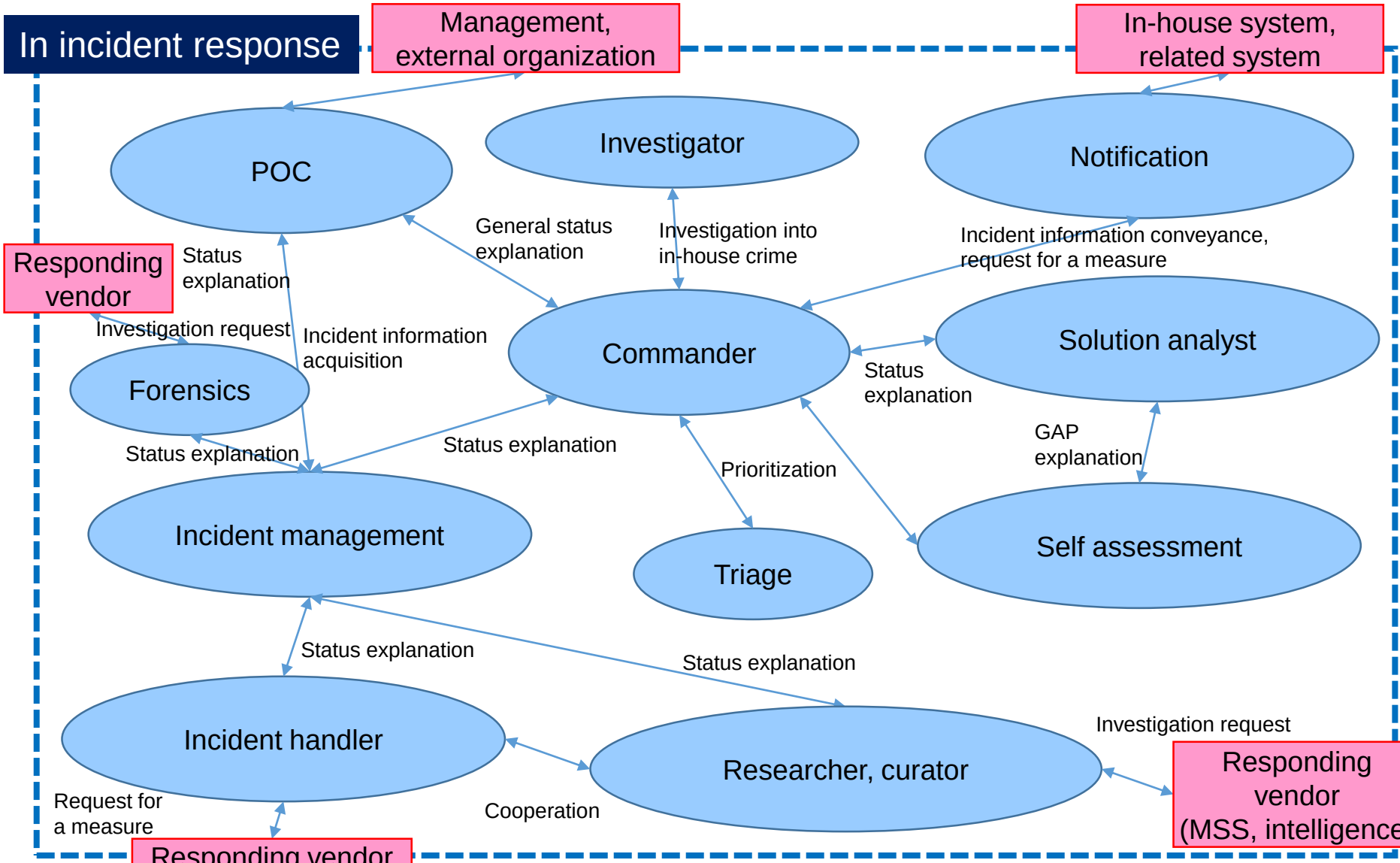
Designs, builds, operates, and maintains the infrastructure system.

Application specialist

Designs, builds, operates, and maintains the application system.

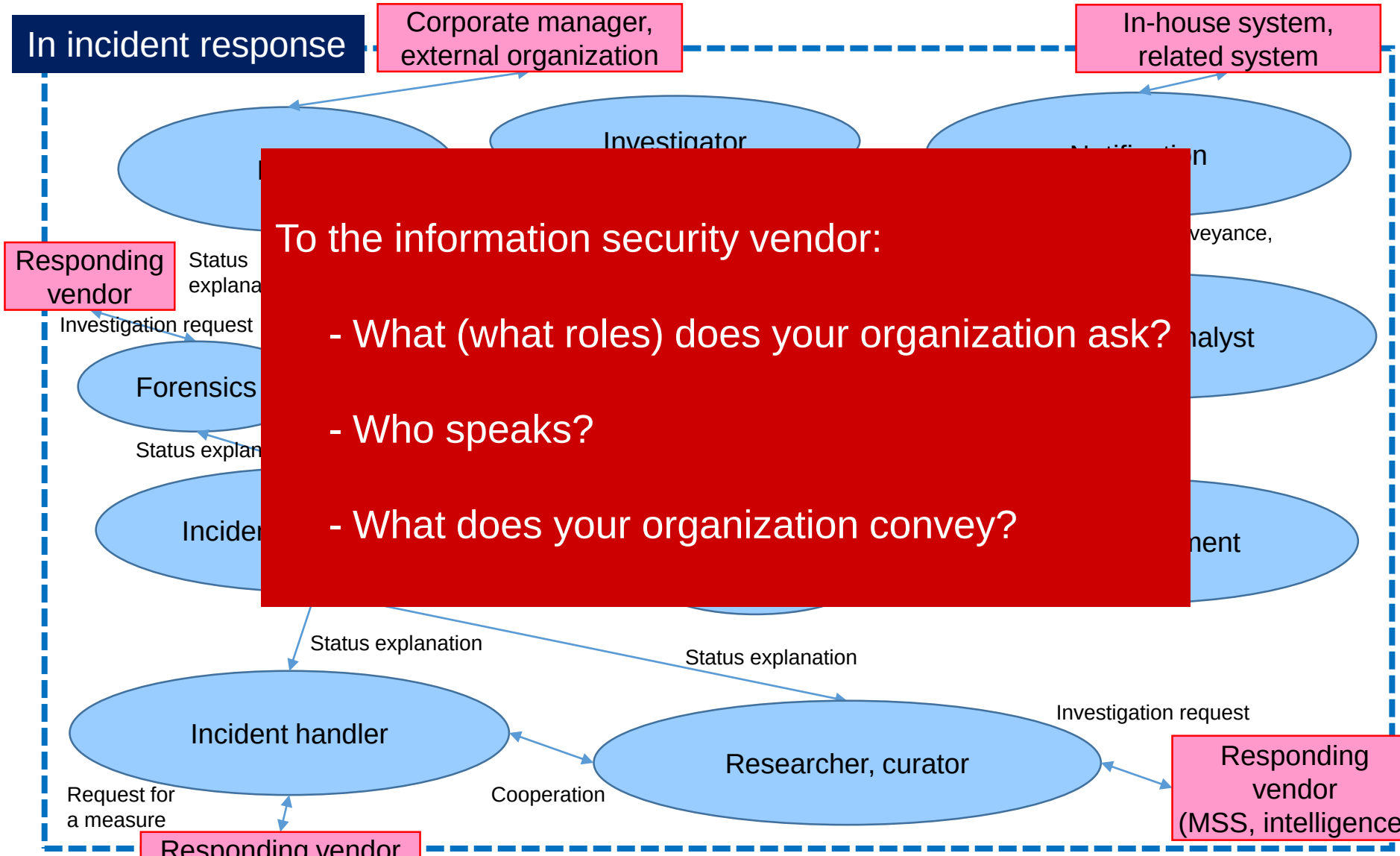
(Reference) Roles of Information Security Engineers in User Companies in Japan and Related Departments

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



(Reference) Roles of Information Security Engineers in User Companies in Japan and Related Departments

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



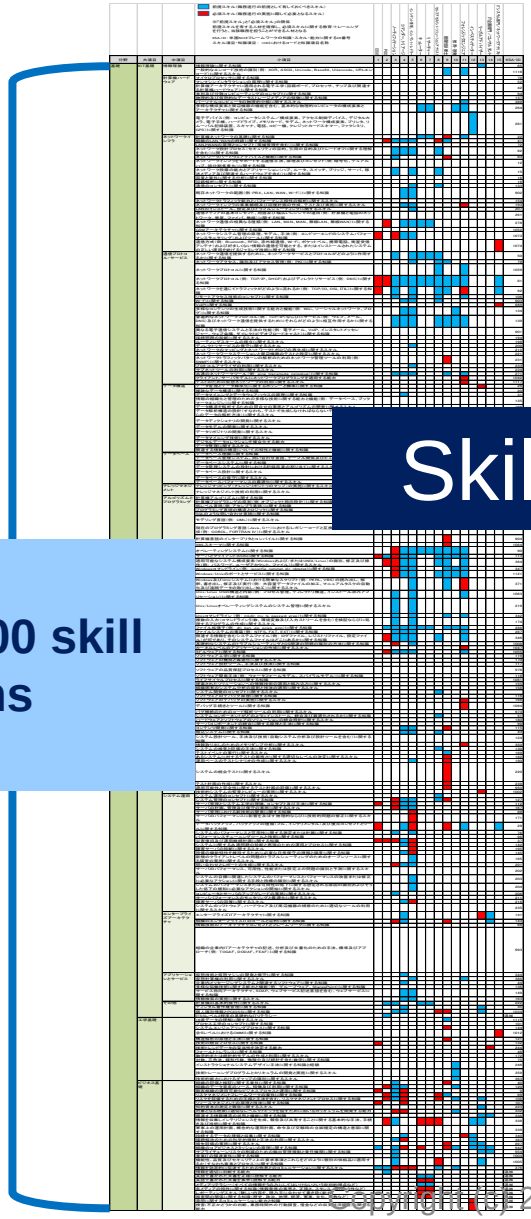
Relationship Example Between Roles and the NICE Framework

Role definition by Nippon CSIRT Association		NICE Specialty Field		User Company Job Type	Security Vendor Job Type
a	CISO	23	Security program management (CISO)	(Board member)	
b	POC		(None)	IT security department	
c	Notification		(None)		
d	Commander	21	Information system security operation (ISSO)		
e	Triage	21	Information system security operation (ISSO)		
f	Incident management	15	Incident response		Incident handler
g	Incident handler	15	Incident response		Incident handler
h	Curator	14 15	Computer network protection analysis Information assurance compliance		SOC analyst
i	Researcher	14	Computer network protection analysis		SOC analyst
j	Solution analyst	13	System security analysis		Malware analyst/ professional sales
k	Self assessment	13	System security analysis		Malware analyst/consultant
l	Vulnerability diagnosis	17	Vulnerability assessment and management		Penetration tester
m	Education/Enlightenment	20	Education and training		(Education service)
n	Forensics	18	Digital forensic		Forensic analyst
o	Investigator	19	Investigation		Forensic analyst
p	(None)	22	Legal advice and defense	(Legal department)	(Lawyer)
q	(None)	24	Formulating strategy and developing policy	(IT planning department)	Consultant
r	(None)	16	Infrastructure support for computer network protection	IT system department	Network analyst

16 Roles of SecBoK

1. CISO (Chief Information Security Officer)
2. POC (Point of Contact)
3. Notification
4. Commander, triage
5. Incident manager, incident handler
6. Curator
7. Researcher
8. Self assessment/solution analyst
9. Vulnerability examiner
10. Education/enlightenment
11. Forensic engineer
12. Investigator
13. Legal adviser
14. IT planning department/consultant
15. IT system department/network analyst
16. Information security auditor

SecBoK (Skill and Roles)



Skill items

Nearly 400 skill items

Classified into 16 roles

Roles

Features of SecBoK2017

1. Support for use in user companies
   SecBoK2017 should be able to support use in user companies, where information security human resources are considerably short in number in Japan.
   -> Coordination with the human resource definition used by Nippon CSIRT Association and mapping to the security vendors are done.

2. Response to world standards
   Frameworks that are not only recognized by JNSA but also publicly acknowledged should be incorporated.
   -> Incorporating the knowledge items related to cyber security in the NICE Framework of NIST

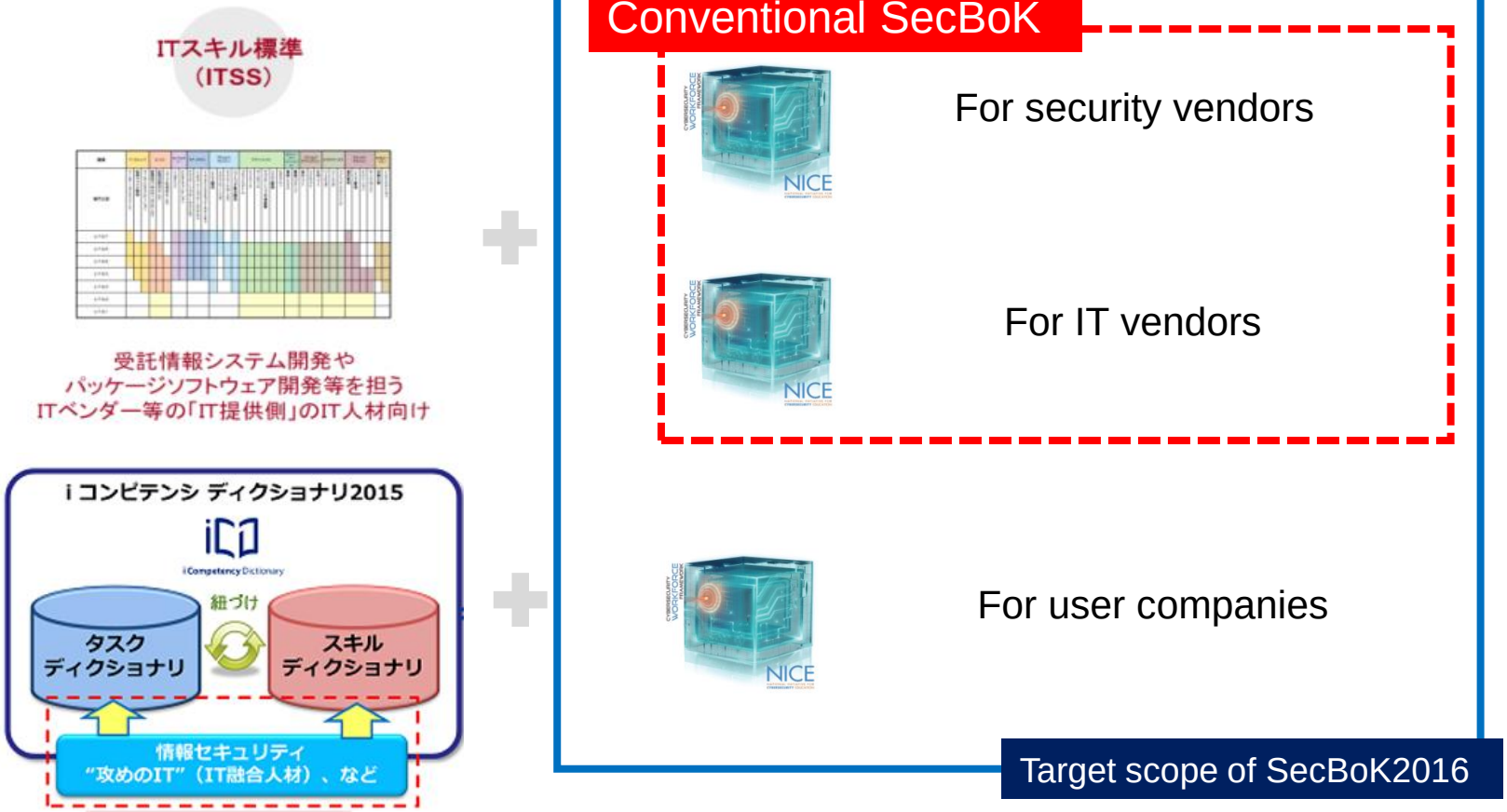
3. Support for organizations/business
   SecBoK2017 should not be too detailed, and should be one from which the actual business flow and organization model can be assumed.
   -> The 32 job types included in the conventional SecBoK are summarized and reduced to 16 job types. Also, coordination with IT skill standards such as i Competency Dictionary and ITSS+ released by IPA is strengthened.

4. How Do We Use SecBoK?

Examples of Using SecBoK

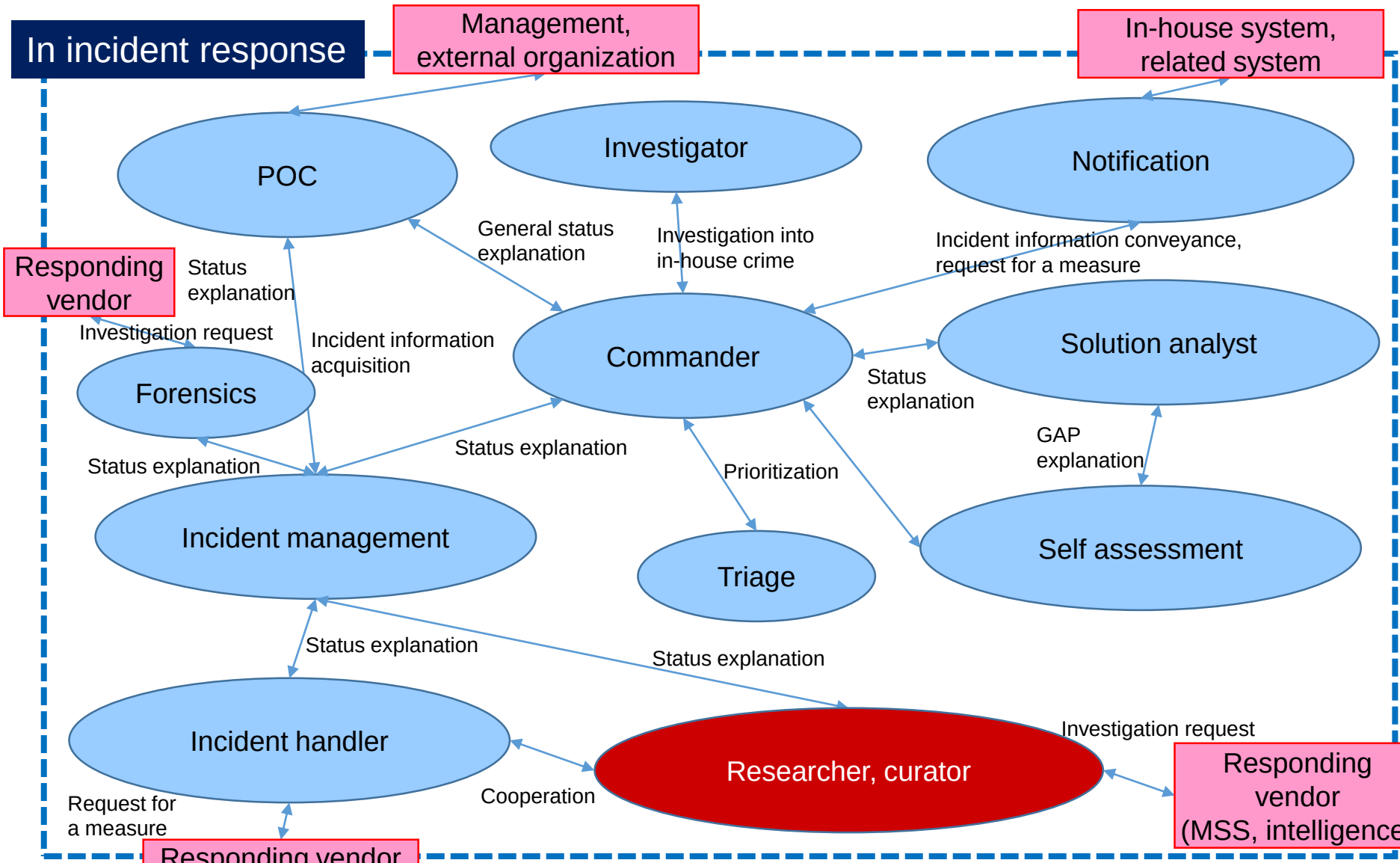
User Companies are Targeted in SecBoK2016

Elements of the framework "NICE," which was considered to be at the world standard level in the context of security, were added to i Competency Dictionary 2015 (former IT Skill Standard) intended for general IT. Then, this i Competency Dictionary with the "NICE" elements being added to was released as Information Security Body of Knowledge (SecBoK).



Example of Developing/Recruiting Researchers and Curators

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



NICE Framework: Example of Mapping With Skill Items

Field	Major Item	Middle Item	KSA-ID	Minor Item	CISO	POC	Notification	Commander/Triage	Incident Management/Incident Handler	Curator	Researcher	Solution Analyst	Vulnerability Examiner	Education/Enlightenment	Forensic Engineer	Investigator	Legal Adviser	Consultant	Network Analyst	Information Security Auditor
Basics of Security	General Description		64	Knowledge on principles of information security system engineering			■			■	■									■
			63	Knowledge on information assurance principles and organization requirements regarding confidentiality, integrity, availability, authentication and non-repudiation			■	■	■	■	■	■	■	■			■	■	■	■
			55	Knowledge on information assurance principles used for managing risks regarding use, processing, accumulation, and transfer of information or data	■	■	■	■	■	■	■						■			■
			70	Knowledge on security principles and methods of information technology (examples: firewall, demilitarized zone, and encryption)			■	■	■	■	■	■	■	■			■			■
			77	Knowledge on methods of the current industry that use concepts and capability based on standards regarding the evaluation, implementation, and popularization of tools and procedures for security assessment, observation, detection, and		■	■	■	■	■	■		■				■			■
			15	integrity, and availability			■	■				■					■			■
			30	hardware, OS, and network			■								■		■			■
			320	Knowledge on external organizations and academic institutions relating to cyber security issues		■	■	■		■	■			■			■	■		■
			952	Knowledge on security problems, risks, and vulnerability that come to the surface		■	■	■	■					■			■			■
Security Governance	General Description		38	Knowledge on the company information security architecture system of organizations			■	■	■			■	■				■			■
			300	Knowledge on reporting principles, policies, procedures, and means (reporting format, report standard (example: requirements and priority)), practice of diffusion and law enforcement agencies, and restrictions of intelligence			■									■	■			■
			965	Knowledge on approach for risk acceptance and/or risk management of organizations		■	■	■				■					■			■

Skill items a little less than 400

Skill map sample - Curator role

Field	Large Category	Middle Category	Small Category	Prerequisite Skill	Required Skill	KSA-ID
Basics of security	General description		Know ledge on principles of information security system engineering	●		64
			Know ledge on information assurance principles and organization requirements regarding confidentiality, integrity, availability, authentication and non-repudiation	●		63
			Know ledge on information assurance principles used for managing risks regarding use, processing, accumulation, and transfer of information or data	●		55
			Know ledge on security principles and methods of information technology (examples: firew all, demilitarized zone, and encryption)	●		70
			Know ledge on methods of the current industry that use concepts and capability based on standards regarding the evaluation, implementation, and popularization of tools and procedures for security assessment, observation, detection, and improvement of information technology	●		77
			Know ledge on external organizations and academic institutions relating to cybersecurity issues		●	320
Security management	General description		Know ledge on security management		●	110
			Know ledge on policies, procedures, and regulations for computer netw ork defense (CND)	●		984
			Know ledge on security policy (such as account creation, passw ord rules, and access control) possessed by those w ho use information technology to take their organizational parts	●		986
			Know ledge on in-house security policies and rules and their implementation methods, etc.		●	Added to SecBoK
			Know ledge on security measures and techniques that are internally implemented		●	Added to SecBoK
Netw ork security	General description		Know ledge on netw ork security architecture concepts (example: defense-in-depth applications) including topology, protocols, components, and principles		●	1072
	Vulnerability diagnosis		Know ledge on know n vulnerabilities that can be obtained from alerts, advisories, and reports		●	58
			Know ledge on computer netw ork defense (CND) and vulnerability evaluation tools (including open-source tools and their capabilities)		●	19
			Skills regarding implementation of vulnerability scanning on security systems and recognition of vulnerabilities involved in security systems		●	3
	VPN		Know ledge on VPN security	●		148

With 15 other roles

5. Key Points of SecBoK 2019 Revisions

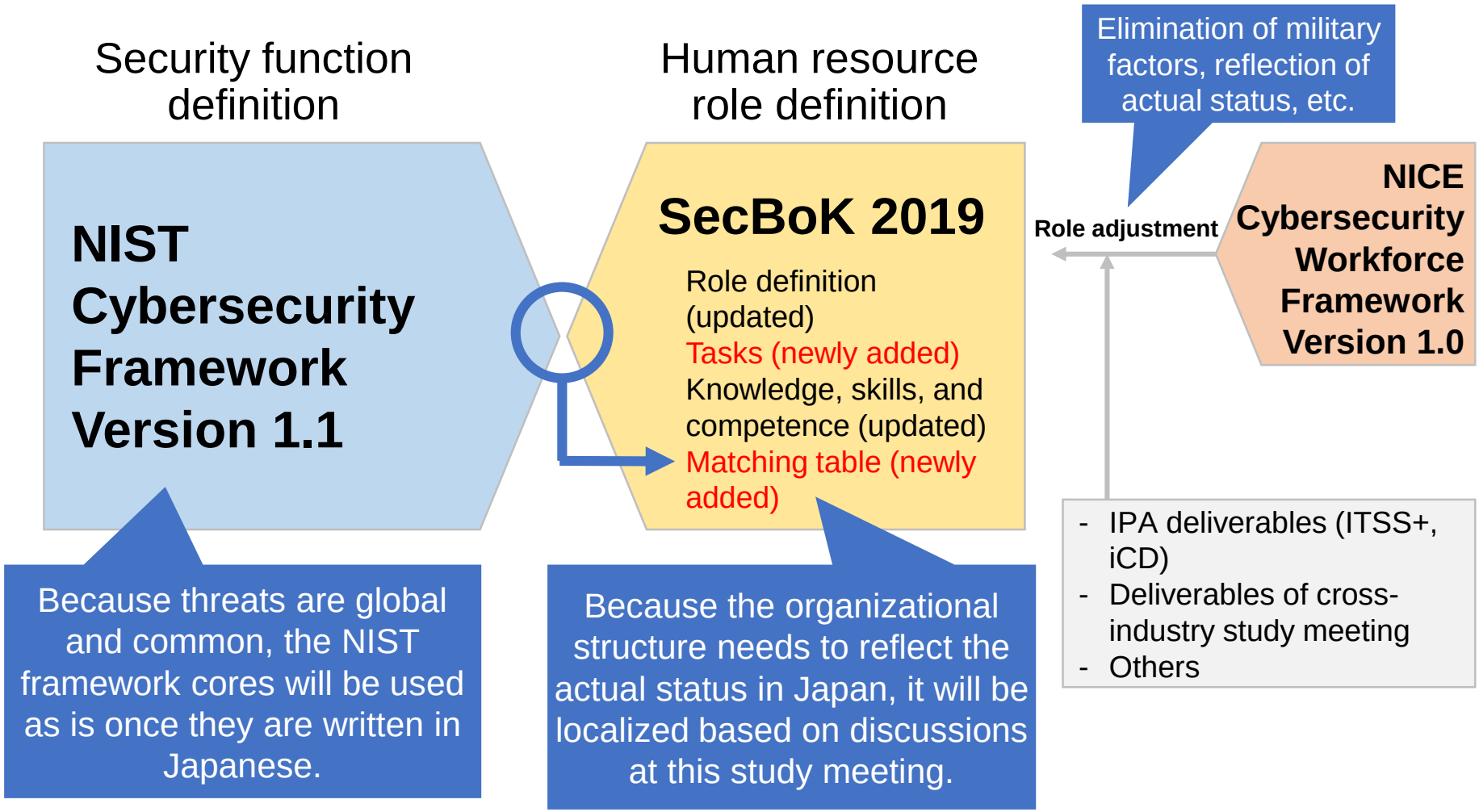
NICE Cybersecurity Workforce Framework

- Standardized as NIST SP800-181 (August 2017)
  - The old version was a document available only as a pamphlet.
  - An Excel version has been also released (January 2018).

- Tasks and skills covered in seven categories
  - Neither the Analyze category nor the Collect & Operate category were provided in the old version because they were unique and highly specialized.
  - Terminology has been reorganized (e.g., information assurance -> cybersecurity).

- Organized into specialty areas
  - The 52 Work Roles are the defined types of cybersecurity roles in government agencies and private services. Individual tasks and the knowledge, skills, and abilities (KSAs) required to perform the tasks are organized into these roles.

Analysis of Security Function and Role Definitions



6. Overview of SecBoK 2019

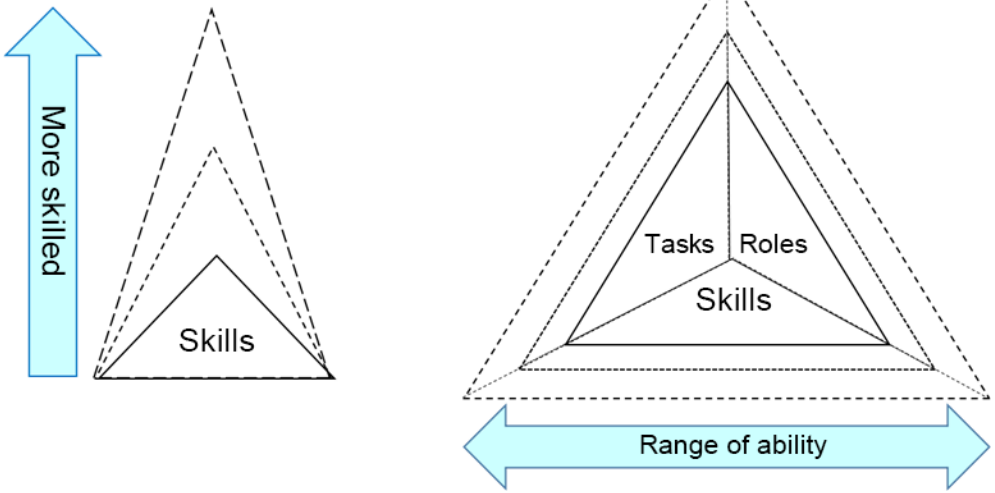
Changing Thinking on Security Human Resource Development From a Focus on Skill to Better Coordination With Tasks and Roles

Traditional Thinking

From a belief that the acquisition of security skills led to the development of security human resources, measures to improve security skills were implemented one after another.

New Way of Thinking

In an era when the effective use of IT is transforming society to Society 5.0 or the like, the objective is not just to acquire security skills. People need to also think about tasks by asking what can be done.



The left diagram illustrates the traditional focus on skill development. These days, however, **skills, tasks, and roles** must be developed to expand their ranges so that the entire triangle becomes larger, as shown in the right diagram.

Features of SecBoK 2019 (1)
NIST SP800-181 Coordination 1

Over 1,000 skills in NIST SP800-181 were coordinated with 16 roles in SecBoK 2019. (Category changes, itemization of the basics, general descriptions, etc., and other work was done independently to facilitate use in Japan.)

Roles

Skills

セキュリティ知識分野（SecBoK）人材スキルマップ2019年版 全体整理表

＜ロール毎の必須知識・スキル＞

1	前提スキル（職務遂行の前提として有しておくべき知識・スキル）
2	必須スキル（職務遂行の実施に際して必要となる知識・スキル）
3	参考スキル（職務遂行に際して必須ではないが、あると望ましい知識・スキル）

※「前提スキル」と「必須スキル」の関係
前提スキルを有する人材を確保し、必須スキルに関する教育・トレーニングを行うと、当該職務を担うことができる人材となる

＜知識・スキルのレベル＞

L	低（概ね経験3年未満でも対応可能）
M	中（経験3年以上または関連する演習・トレーニング受講者なら対応可能）
H	高（経験10年以上または高度な研修受講を前提とする専門実務経験者または「突出した人材」なら対応可能）
P	ペンディング（情報収集・インテリジェンスに関するもの。今回はレベル付けの対象外）

	KSA-ID	New/Old	Old ID	Field	Major Item	Middle Item	Level	Minor Item	CISO	POC	Notification	Commander/Triage	Incident Manager/Incident Handler	Curator	Researcher	Self Assessment/Solution Analyst	Vulnerability Examiner	Education/Enlightenment	Forensic Engineer	Investigator	Legal Adviser	IT Planning Department	IT System Department	Information Security Auditor
1	K0052	旧NICEに類似項あり	75	00基礎	1数物情報学		L	数学に関する知識（例：対数、三角法、線形代数、微積分、統計、操作解析）								3								
2	K0030	旧NICEに類似項あり	42	00基礎	2計算機・通信工学		L	コンピュータアーキテクチャ（例：回路基板、プロセッサ、チップ及びコンピュータハードウェア）に適用される電気工学に関する知識																	
3	K0036	旧NICEと同一	52	00基礎	2計算機・通信工学		L	マンマシンインタラクションの原理に関する知識						1		1								
4	K0055	旧NICEと同一	78	00基礎	2計算機・通信工学		L	マイクロプロセッサに関する知識																
5	K0061	旧NICEとほぼ同一	92	00基礎	2計算機・通信工学		L	ネットワーク上でトラフィックがどのように流れるか（例：TCP/IP、OSI、ITIL現行版）に関する知識	2		1		1		1	1	1		1				1	
6	K0108	旧NICEに類似項あり	261	00基礎	2計算機・通信工学		L	通信メディアの基本概念、用語及び幅広い範囲での運用に関する知識（コンピュータと電話のネットワーク、衛星、ファイバ、無線）						3									1	
7	K0109	旧NICEに類似項あり	264	00基礎	2計算機・通信工学		L	多様な構成要素と周辺機器の機能を含む、物理的なコンピュータの構成要素とアーキテクチャに関する知識（例：CPU、ネットワークインターフェースカード、データストレージ）の機能を含む、物理的なコンピュータコンポーネントとアーキテクチャに関する知識						1	1			1	1					
8	K0113	旧NICEとほぼ同一	278	00基礎	2計算機・通信工学		L	さまざまな種類のネットワーク通信に関する知識（例：LAN、WAN、MAN、WLAN、WWAN）		2		1	1	1	1								1	
9	K0114	旧NICEとほぼ同一	281	00基礎	2計算機・通信工学		L	電子デバイスに関する知識（例：コンピュータシステム/コンポーネント、アクセス制御デバイス、デジタルカメラ、デジタルスキャナ、電子オーガナイザ、ハードドライブ、メモリカード、モデム、ネットワークコンポーネント、ネットワークアプライアンス、ネットワークホームコントロールデバイス、プリンタ、リムーバブルストレージデバイス、電話機、複写機、ファクシミリなど）											3					
10	K0138	旧NICEに類似項あり	903	00基礎	2計算機・通信工学		L	Wi-Fiに関する知識				1	1			1							1	
11	K0395	旧NICEとほぼ同一	22	00基礎	2計算機・通信工学		L	コンピュータネットワークの基礎に関する知識（ネットワークの基本的なコンピュータコンポーネント、ネットワークの種類など）						1	1		1		1					1
12	K0491	新規	—	00基礎	2計算機・通信工学		L	ネットワークとインターネット通信に関する知識（すなわち、デバイス、デバイス構成、ハードウェア、ソフトウェア、アプリケーション、ポート/プロトコル、アドレッシング、ネットワークアーキテクチャとインフラストラクチャ、ルーティング、オペレーティングシステムなど）					1	1	1	1	1		1			1	1	1
13	K0516	新規	—	00基礎	2計算機・通信工学		L	ハブ、スイッチ、ルータ、ファイアウォールなどを含む物理的および論理的なネットワークデバイスおよびインフラストラクチャに関する知識					1	1	1	1	1		1			1	1	1
14	K0555	新規	—	00基礎	2計算機・通信工学		L	TCP/IPネットワーキングプロトコルに関する知識					1	1	1	1	1		1			1	1	1
15	K0556	新規	—	00基礎	2計算機・通信工学		L	通信の基礎に関する知識					1	1	1	1	1		1			1	1	1
16	K0015	旧NICEと同一	21	00基礎	3ソフトウェア		L	計算機アルゴリズムに関する知識						1	1	1	1		1					
17	K0016	旧NICEに類似項あり	23	00基礎	3ソフトウェア		L	コンピュータプログラミングの原則に関する知識						1	1	1	1		1					

Features of SecBoK 2019 (2)
NIST SP800-181 Coordination 2

	Role	Defined Role (Main Role in User Company)	Role Name in NICE Definitions		Role Defined by NICE
1	CISO (Chief Information Security Officer)	社内の情報セキュリティを統括する。セキュリティ確保の観点から、CIO（最高情報セキュリティ責任者）、CFO（最高財務責任者）と必要に応じて対峙する。	1	Authorizing official	組織の業務（ミッション、機能、イメージ、評判を含む）、組織資産、個人、その他の組織、国家に許容可能なレベルで情報システムを運用する責任を正式に負う権限を持つ上級管理職または役員。
			27	Executive cyber leadership	組織のサイバーおよびサイバー関連の資源及び/又は運用に関する意思決定を行うとともに、ビジョンと方向性を確立する。
			31	IT investment/portfolio manager	ミッションと企業の優先度に関する全体的なニーズに合わせたIT投資のポートフォリオを管理する。
2	POC (Point of Contact)	社外向けではJPCERT/CC、NISC、警察、監督官庁、NCA、他CSIRT等との連絡窓口、社内向けではIT部門調整担当社内の法務、渉外、IT部門、広報、各事業部等との連絡窓口となり、それぞれ情報連携を行う。		(No response role)	
3	Notification	組織内を調整し、社内各関連部署への情報発信を行う。社内システムに影響を及ぼす場合にはIT部門と調整を行う。		(No response role)	
4	Commander	自社で起きているセキュリティインシデントの全体統制を行う。重大なインシデントに関してはCISOや経営層との情報連携を行う。また、CISOや経営者が意思決定する際の支援を行う。	27	Executive cyber leadership	組織のサイバーおよびサイバー関連の資源及び/又は運用に関する意思決定を行うとともに、ビジョンと方向性を確立する。
4	Triage	事象に対する対応における優先順位を決定する。	27	Executive cyber leadership	組織のサイバーおよびサイバー関連の資源及び/又は運用に関する意思決定を行うとともに、ビジョンと方向性を確立する。
5	Incident manager	インシデントハンドラーに指示を出し、インシデントの対応状況を把握する。対応履歴を管理するとともにコマンダーへ状況を報告する。	35	Cyber defense incident responder	ネットワーク環境またはエンクレーブ内のサイバーインシデントを調査、分析、および対応する。
5	Incident handler	インシデントの処理を行う。セキュリティベンダーに処理を委託している場合には指示を出して連携し、管理を行う。状況はインシデントマネージャーに報告する。	35	Cyber defense incident responder	ネットワーク環境またはエンクレーブ内のサイバーインシデントを調査、分析、および対応する。
6	Curator	リサーチャーの収集した情報を分析し、その情報を自社に適用すべきかの選定を行う。リサーチャーと合わせてSOC（セキュリティオペレーションセンター）とすることが多い。	37	Threat/Warning analyst	高度にダイナミックなオペレーティング環境の状況を把握するためのサイバー指標を開発する。サイバー脅威/警告評価を収集、処理、分析、および普及させる。
7	Researcher	セキュリティイベント、脅威情報、脆弱性情報、攻撃者のプロファイル情報、国際情勢の把握、メディア情報などを収集し、キュレーターに引き渡す。収集のみで分析はしない。	33	Cyber defense analyst	さまざまなサイバー防御ツール（IDSのアラート、ファイアウォール、ネットワークトラフィックログなど）から収集したデータを使用して、脅威を緩和する目的で環境内で発生するイベントを分析する。
8	Self-assessment	自社の事業計画に合わせてセキュリティ戦略を策定する。現在の状況とTobe像のFit&Gapからリスク評価を行い、ソリューションマップを作成して導入を推進する。導入されたソリューションの有効性を確認し、改善計画に反映する。	18	System security analyst	システムセキュリティの統合、テスト、運用、保守の分析と開発を担当する。
8	Solution analyst	平常時にはリスクアセスメントを行う。インシデント対応時には脆弱性の分析、影響の調査等に対応する。	18	Systems security analyst	システムセキュリティの統合、テスト、運用、保守の分析と開発を担当する。
9	Vulnerability examiner	ネットワーク、OS、ミドルウェア、アプリケーションがセキュアプログラミングされているかどうかの検査を行い、診断結果の評価を行う。	36	Vulnerability assessment analyst	ネットワーク環境内のシステムとネットワークの評価を実施し、それらのシステム/ネットワークが受け入れ可能な構成、特殊又はローカルなポリシーから逸脱している場所を特定する。既知の脆弱性に対する多層防御アーキテクチャの有効性を評価する。
10	Education/ Enlightenment	社内のリテラシーの向上、底上げのための教育及び啓発活動を行う。	21	Cyber instructional curriculum developer	教育上の必要に基づき、サイバーセキュリティを対象とする訓練・教育に関するコース、手法及び技術について開発、立案、調整及び評価する。
			22	Cybersecurity instructor	サイバーセキュリティ領域における要員の訓練または教育を開発及び主導する。
			25	Cyber workforce developer and manager	サイバー空間の人材、人材、訓練、教育の要件をサポートし、サイバー関連のポリシー、原則、教材、編成、教育訓練の要件に対する変化を扱うためのサイバー空間を対象とする労働力の計画、戦略、指針を開発する。
11	Forensic engineer	システム的な鑑識、精密検査、解析、報告を行う。悪意のある者は証拠隠滅を図ることもあるため、証拠保全とともに、消されたデータを復活させ、足跡を追跡することも要求される。	51	Law enforcement forensics analyst	サイバー侵入事件に関連するデジタルメディアとログを含めるために、ドキュメンタリーまたは物理的証拠を確立するコンピュータベースの犯罪に関する詳細な調査を実施する。
			52	Cyber defense forensics analyst	デジタル証拠を分析し、コンピュータセキュリティインシデントを調査し、システム/ネットワークの脆弱性緩和を支援する有益な情報を導き出す。
12	Investigator	外部からの犯罪、内部犯罪を捜査する。セキュリティインシデントはシステム障害とは異なり、悪意のある者が存在する。通常の犯罪捜査と同様に、動機の確認や証拠の確保、次に起こる事象の推測などを詰めながら論理的に捜査対象を絞っていくことが要求される。	50	Cyber crime investigator	制御され、文書化された分析および調査技術を使用して、証拠を特定、収集、調査、および保存する。
13	Legal adviser	システムにおいてコンプライアンス及び法的観点から遵守すべき内容に関する橋渡しを行う。	19	Cyber legal adviser	サイバー法に関するトピックについて、法的な助言や勧告を行う。
14	IT planning department	社内のIT利用に関する企画・立案を行う。必要に応じて、ITの利用状況の調査・分析等を行う。	26	Cybersecurity policy and strategy planner	組織のサイバーセキュリティに関するイニシアチブおよび規制遵守をサポートし、それと整合するようなサイバーセキュリティ計画、戦略、およびポリシーを策定し維持する。
			29	IT project manager	情報技術関連プロジェクトを直接管理する。
15	IT system department	社内のITプロジェクトを推進するとともに、アプリケーションシステムの設計、構築、運用、保守等を担当する。	16	Network operations specialist	ハードウェアおよび仮想環境を含む、ネットワークサービス/システムの計画、実装、および運用を行う。
			17	System administrator	システムまたはシステムにおける特定のコンポーネントの設定および保守（例：ハードウェアおよびソフトウェアのインストール、構成、更新、ユーザーアカウントの確立および管理、バックアップおよびリカバリタスクの監督または実施、運用上および技術上のセキュリティ管理の実装、組織のセキュリティポリシーと手順への準拠）に関する責任を負う。
			23	Information systems security manager	プログラム、組織、システム等におけるサイバーセキュリティ対策に責任を負う。
			24	Communications security manager	組織の通信リソースまたは暗号鍵管理システムの鍵を管理する。
			34	Cyber defense infrastructure support specialist	インフラストラクチャのハードウェアとソフトウェアをテスト、実装、展開、保守、管理する。
16	Information security auditor	情報セキュリティに係るリスクのマネジメントが効果的に実施されるよう、リスクアセスメントに基づく適切な管理策の整備、運用状況について、基準に従って検証又は評価し、もって保証を与えあるいは助言を行う。	32	IT program auditor	標準への準拠状況を判断するため、ITプログラムまたはその個々の構成要素を評価する。

Among the 52 roles in NIST SP800-181, associated roles were picked out and coordinated with the 16 roles in SecBoK 2019.

Features of SecBoK 2019 (3)
NIST Cybersecurity Framework (CSF) Coordination

Unique Function Identifier	Function
ID	Identify
PR	Protect
DE	Detect
RS	Respond
RC	Recover

Tasks are coordinated with knowledge items in newly presented tables.
An example of the Detect (DE) task is shown below.

Knowledge items (skills)

			Basics	Security Basics	Security Governance	Security Management	Network Security	System Security	Secure System Design and Build	Security Operation	Cryptography, Authentication, Electronic Signature	Cyber Attack Vector	Information Collection Intelligence	Digital Forensics	Cyber Investigation	Security Human Resource Development	Laws, Regulatory System, Standards	Related Areas (No H Level) IOT	Engineering	Business	Education
検知（DE	異常とイベント(DE.AE): 異常な活動を検知し、イベントがもたらす可能性のある影響を把握している。	DE.AE-1: ネットワーク運用のベースラインと、ユーザとシステム間の予測されるデータの	•	•		L	H			M	L	M					L	L			
		DE.AE-2: 攻撃の標的と手法を理解するために、検知したイベントを分析している。	•	•		L	H	H	M	H	M	H		L	L		L	L	L	L	
		DE.AE-3: イベントデータを複数の情報源やセンサーから収集し、相互に関連付けている。	•	•		L	H	M	M	H	M	H		L	L		L	L	L	L	
		DE.AE-4: イベントがもたらす影響を特定している。	•	•		L	H	H	H	H	M	H		L	L		L	L	L	L	
		DE.AE-5: インシデント警告の閾値を定めている。	•	•	L	M	H	H	M	H	M	H		L	L		M	L	L	M	
	セキュリティの継続的なモニタリング(DE.CM): サイバーセキュリティイベントを検知し、保護対策の有効性を検証するために、情報システムと資産をモニタリングしている。	DE.CM-1: 発生する可能性のあるサイバーセキュリティイベントを検知できるよう、ネッ	•	•		L	M	M		M		H						L		L	
		DE.CM-2: 発生する可能性のあるサイバーセキュリティイベントを検知できるよう、物理環境をモニタリングしている。	•	•		L	M	M		M		H						L		L	
		DE.CM-3: 発生する可能性のあるサイバーセキュリティイベントを検知できるよう、個人の活動をモニタリングしている。	•	•		L	M	M		M		M		L	L			L	L	M	
		DE.CM-4: 悪質なコードを検出できる。	•	•			H	H		M		H		L	L			L	L	L	
		DE.CM-5: 悪質なモバイルコードを検出できる。	•	•			H	H		M		H		L	L			L	L	L	
		DE.CM-6: 発生する可能性のあるサイバーセキュリティイベントを検知できるよう、外部サービスプロバイダの活動をモニタリングしている。	•	•		M	M	L		H		H						L	L	L	
		DE.CM-7: 権限のない従業員、接続、デバイス、ソフトウェアのモニタリングを実施している。	•	•		M	L	L		H		M		L	L			L	L	L	
		DE.CM-8: 脆弱性スキャンを実施している。	•	•			M	M		M		H		L				L	L		
	検知プロセス(DE.DP): 異常なイベントを検知するための検知プロセスおよび手順を維持し、テストしている。	DE.DP-1: 説明責任を果たせるよう、検知に関する役割と責任を明確に定義してい	•	•	L	H	M	M	L	H	L	H		L			M	L	L	L	
		DE.DP-2: 検知活動は必要なすべての要求事項を満たしている。	•	•		H				H		H		L			M	L	L	L	
		DE.DP-3: 検知プロセスをテストしている。	•	•		M	H	H	M	H	L	H		L			M	L	L	L	
		DE.DP-4: イベント検知情報を伝達している。	•	•	L	H				M		M					L	L	L	M	
		DE.DP-5: 検知プロセスを継続的に改善している。	•	•		H				M		M					L	L	L	M	

Features of SecBoK 2019 (4)
Reference: List of Human Resources and Tasks Defined by NICE

SecBok publishes a Japanese version of the list of tasks performed by the human resources involved in each role defined by NICE (NIST SP800-181).

システムアーキテクチャ Systems Architecture (ARC)	SP-ARC-001 エンタープライズアーキテクト Enterprise Architect	T0051	重要なシステム機能に基づいて適切なレベルのシステム可用性を定義し、適切なフェールオーバー/代替サイト要件、バックアップ要件、システム復旧/復元のためのマテリアルサポート性要件を含む適切な災害復旧と運用要件の継続性を、システム要件が確実に識別するようにする。
		T0084	安全な構成管理プロセスを採用する。
		T0090	取得または開発されたシステムとアーキテクチャが、組織のサイバーセキュリティアーキテクチャガイドラインと一貫していることを確認する。
		T0108	組織のステークホルダーと連携して重要なビジネス機能を特定し、優先順位を付ける。
		T0196	プロジェクト費用、設計コンセプト、または設計変更に関するアドバイスを提供する。
		T0205	リスク管理フレームワークのプロセス活動および関連する文書（例えば、システムライフサイクルサポート計画、運用の概念、運用手順、および保守トレーニング資料）を入力する。
		T0307	候補アーキテクチャの分析、セキュリティサービスの割り当て、セキュリティメカニズムの選択を行う。
		T0314	システムセキュリティコンテキスト、予備システムセキュリティコンセプト（CONOPS）を開発し、適用可能なサイバーセキュリティ要件に従ってベースラインシステムセキュリティ要件を定義する。
		T0328	セキュリティアーキテクチャと設計を評価して、取得文書に含まれる要件に応じて提案または提供されるセキュリティ設計とアーキテクチャの妥当性を判断する。
		T0338	アーキテクチャ開発プロセスを記述する詳細な機能仕様を記述する。
		T0427	アーキテクチャを計画するためのユーザーのニーズと要件を分析する。
		T0440	致命的な障害イベントが発生した後、システムの一部または全部を復旧するために必要なシステム機能やビジネス機能をキャプチャして統合する。
		T0448	ユーザーのニーズを満たすために必要なエンタープライズアーキテクチャまたはシステムコンポーネントを開発する。
		T0473	必要に応じてすべての定義およびアーキテクチャ活動を文書化して更新する。
		T0517	セキュリティアーキテクチャのギャップの特定に関する結果を統合する。
		T0521	企業のコンポーネントを統合して整列させるための実装戦略を立てる。
		T0542	提案された機能を技術要件に変換する。
		T0555	システム間の新しいシステムまたは新しいインターフェースの実装が、セキュリティーの姿勢を含むがこれに限定されない現在の環境およびターゲット環境にどのように影響するかを文書化する。
		T0557	サイバースペースに関連するキー管理機能を統合する。
	SP-ARC-002 セキュリティアーキテクト Security Architect	T0050	致命的な障害イベントが発生した後、システムの一部または全部を復旧するために必要なシステム機能またはビジネス機能を定義し、優先順位を付ける。
		T0051	重要なシステム機能に基づいて適切なレベルのシステム可用性を定義し、適切なフェールオーバー/代替サイト要件、バックアップ要件、システム復旧/復元のためのマテリアルサポート性要件を含む適切な災害復旧と運用要件の継続性を、システム要件が確実に識別するようにする。
		T0071	主に政府組織に適用される複数の分類レベルのデータ（UNCLASSIFIED、SECRET、およびTOP SECRETなど）の処理のための、複数レベルのセキュリティ要件または要件を備えたシステムおよびネットワークのサイバーセキュリティ設計の開発/統合。
		T0082	取得ライフサイクル全体にわたる組織の情報セキュリティ、サイバーセキュリティアーキテクチャ、およびシステムセキュリティエンジニアリング要件の文書化と処理を行う。
		T0084	安全な構成管理プロセスを採用する。
		T0090	取得または開発されたシステムとアーキテクチャが、組織のサイバーセキュリティアーキテクチャガイドラインと一貫していることを確認する。
		T0108	組織のステークホルダーと連携して重要なビジネス機能を特定し、優先順位を付ける。
		T0177	セキュリティレビューを実行し、セキュリティアーキテクチャのギャップを特定し、セキュリティリスク管理計画を策定する。
		T0196	プロジェクト費用、設計コンセプト、または設計変更に関するアドバイスを提供する。
		T0203	業務声明やその他の適切な調達文書に含めるべきセキュリティ要件に関する情報を提供する。
		T0205	リスク管理フレームワークのプロセス活動および関連する文書（例えば、システムライフサイクルサポート計画、運用の概念、運用手順、および保守トレーニング資料）を入力する。
		T0268	新しいシステムの実装またはシステム間の新しいインターフェイスが現在の環境のセキュリティの姿勢にどのように影響するかを定義し、文書化する。
		T0307	候補アーキテクチャの分析、セキュリティサービスの割り当て、セキュリティメカニズムの選択を行う。
		T0314	システムセキュリティコンテキスト、予備システムセキュリティコンセプト（CONOPS）を開発し、適用可能なサイバーセキュリティ要件に従ってベースラインシステムセキュリティ要件を定義する。
		T0328	セキュリティアーキテクチャと設計を評価して、取得文書に含まれる要件に応じて提案または提供されるセキュリティ設計とアーキテクチャの妥当性を判断する。
		T0338	アーキテクチャ開発プロセスを記述する詳細な機能仕様を記述する。
		T0427	アーキテクチャを計画するためのユーザーのニーズと要件を分析する。
		T0448	ユーザーのニーズを満たすために必要なエンタープライズアーキテクチャまたはシステムコンポーネントを開発する。
		T0473	必要に応じてすべての定義およびアーキテクチャ活動を文書化して更新する。
		T0484	情報システムとネットワークおよび文書の保護ニーズ（すなわち、セキュリティ制御）を適切に決定する。
		T0542	提案された機能を技術要件に変換する。
		T0556	サイバースペースに関連するセキュリティ管理機能を評価し、設計する。

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.

Effective Use of SecBoK in ASEAN Countries Case Examples in Indonesia and Vietnam

The Japan International Cooperation Agency (JICA) has implemented projects for security human resource development using SecBoK.

Indonesia: Project for Human Resources Development for Cyber Security Professionals

https://www2.jica.go.jp/ja/evaluation/pdf/2018_1701288_1_s.pdf (*in Japanese*)

Project Outline

The establishment of a cybersecurity education system for professionals (practitioners) at the University of Indonesia, one of the best universities in Indonesia, will lead to a continuous supply of cybersecurity human resources to private-sector institutions and governments focusing on critical information infrastructures.

Business Outline

This business in Indonesia will establish a cybersecurity program at the University of Indonesia to develop professional human resources in accordance with the Security Body of Knowledge (SecBoK) Human Resource Skill Map. The program will also involve cybersecurity human resources from other countries, enhancing the cybersecurity human resource development system at the university. This will contribute to strengthening the cybersecurity response capabilities of private-sector institutions and governments.

Vietnam: Project on Capacity Building for Cyber Security in Vietnam (Career Development Plan)

https://www2.jica.go.jp/ja/announce/pdf/20190424_190086_4_02.pdf (*in Japanese*)

Project Outline

Vietnam's Ministry of Information and Communications requested the implementation of the Project on Capacity Building for Cyber Security. The requested matters include improvement of the capabilities of government cybersecurity human resources, provision of equipment and technology to protect government information networks against cyber attacks, and activities to raise awareness of cybersecurity.

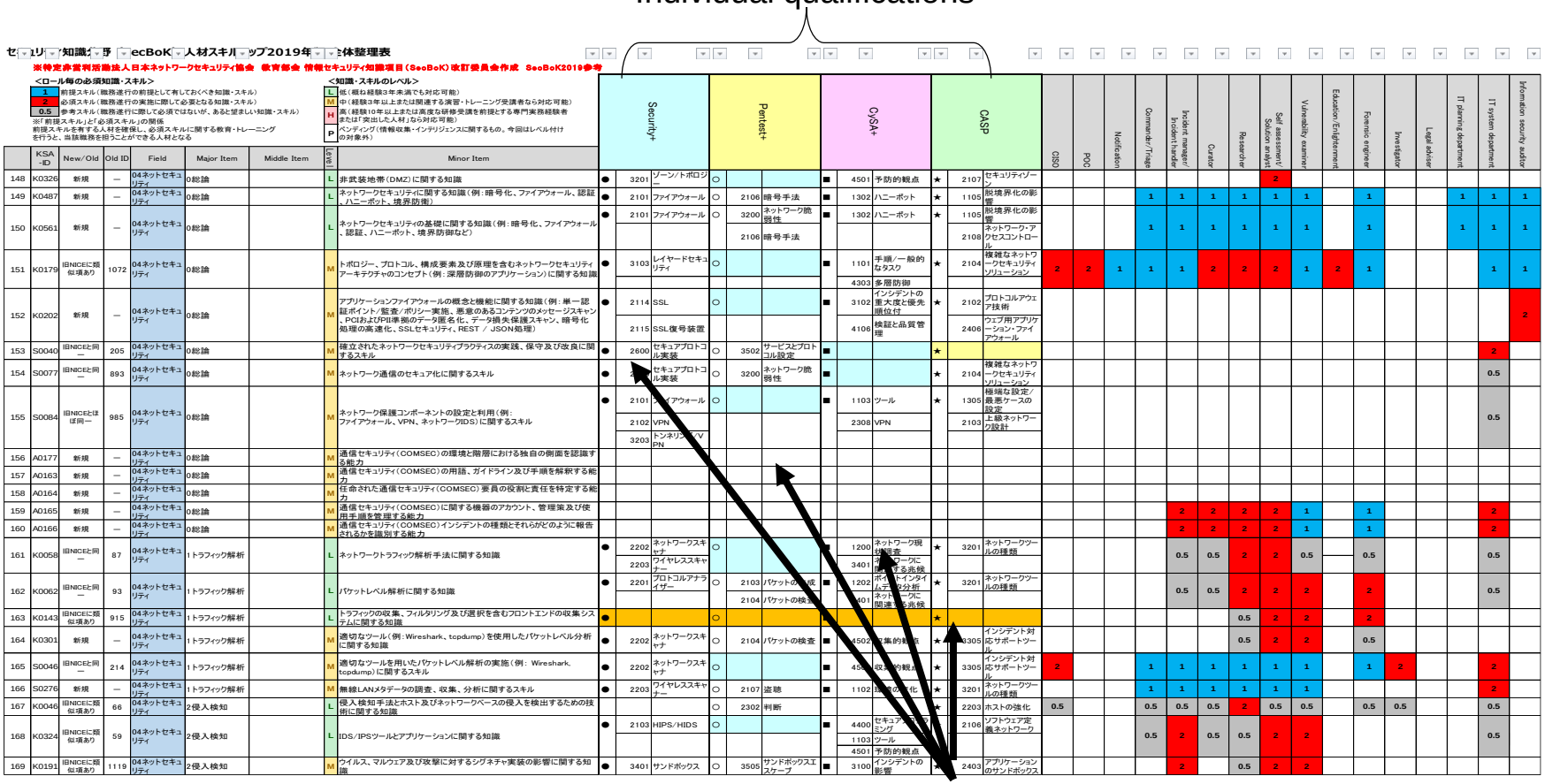
Activity Outline

The activities are to clarify the necessary roles among roles defined in the SecBoK framework, and to establish a career development plan for each official. Another activity is to plan and implement training courses for higher-priority roles among roles defined in the SecBoK framework.

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

Conclusion
Security Human Resource Development: Go to the Next Stage!

1. Does cybersecurity really have a human resource shortage?
   There really is a shortage of human resources but the necessary human resources are changing.
2. How about human resource shortages after the Olympics and Paralympic Games in 2020?
   Even the United States, which has nothing to do with the upcoming Olympics, faces a serious shortage of security human resources.
3. Why is security a management issue?
   Cybersecurity damage is serious and a major risk to the global economy.
4. Security is not a concern for your company.
   Security is a necessity for companies dealing with their digital transformation (DX) in order to survive in the future.
5. Is SecBoK relevant only to security companies?
   SecBoK is useful for the human resource development of not only security specialists but also for human resources who need additional security skills.
6. What is a new stage for security human resource development?
   Traditionally, human resource development of security specialists focuses on skills. In addition to that traditional approach, it is necessary to think about tasks by asking "**What can with security skills do?**" and also to nurture **human resources who need additional security skills** since their business divisions or user companies require security.

SecBoK:
Security
Body
of
Knowledge