（注）
「I-5.セキュリティベンダーとの連携」および「I-6.セキュリティ関連団体との連携」は、実態としては各役割の中で実行されるため、その時の役割と同等のスキルとなる。

			リアルタイム基本分析	リアルタイム高度分析	トリアージ情報収集	リアルタイム分析報告	分析内容問合受付	検体解析	リモート対処	オンサイト対処	ネットワークセキュリティ製品基本運用	ネットワークセキュリティ製品高度運用	エンドポイントセキュリティ製品基本運用	エンドポイントセキュリティ製品高度運用	ディープアナリシス（深掘分析）ツール運用	分析基盤基本運用	分析基盤高度運用	既設セキュリティ対応ツール検証	新規セキュリティ対応ツール調査、開発	内部不正検知・防止支援	セキュリティベンダーとの連携	セキュリティ関連団体との連携
NICE			本紙での役割																			
KSA-ID	Statement	Competency	B-1.	B-2.	B-3.	B-4.	B-5.	C-3.	D-4.	D-5.	G-1.	G-2.	G-3.	G-4.	G-5.	G-6.	G-7.	G-8.	G-9.	H-3.	I-5.	I-6.
154	Skill in analyzing network traffic capacity and performance characteristics.	Capacity Management									○	○									（注）	
114	Knowledge of server diagnostic tools and fault identification techniques.	Computer Forensics														○	○					
340	Knowledge of types and collection of persistent data.	Computer Forensics												○	○							
346	Knowledge of which system files (e.g., log files, registry files, configuration files) contain relevant information and where to find those system files.	Computer Forensics												○	○							
360	Skill in identifying and extracting data of forensic interest in diverse media (i.e., media forensics).	Computer Forensics												○								
888	Knowledge of types of digital forensics data and how to recognize them.	Computer Forensics												○								
1086	Knowledge of data carving tools and techniques (e.g., Foremost).	Computer Forensics												○								
1093	Knowledge of common forensic tool configuration and support applications (e.g., VMware, Wireshark).	Computer Forensics												○								
1099	Skill in analyzing volatile data.	Computer Forensics												○								
74	Knowledge of low-level computer languages (e.g., assembly languages).	Computer Languages						○														
102	Knowledge of programming language structures and	Computer Languages						○														
342	Knowledge of Unix command line (e.g., mkdir, mv, ls, passwd, grep).	Computer Languages	○	○	○	○	○	○	○	○	○	○	○	○		○	○	○	○	○		
904	Knowledge of interpreted and compiled computer languages.	Computer Languages	○	○	○	○	○	○	○	○	○	○	○	○		○	○	○	○	○		
1088	Skill in using binary analysis tools (e.g., Hexedit, command code xxd, hexdump).	Computer Languages	○	○	○	○	○	○	○	○	○	○	○	○		○	○	○	○	○		
1115	Skill in reading Hexadecimal data.	Computer Languages	○	○	○	○	○	○	○	○	○	○	○	○		○	○	○	○	○		
1116	Skill in identifying common encoding techniques (e.g., Exclusive Disjunction [XOR], American Standard Code for Information Interchange [ASCII], Unicode, Base64, Uuencode, Uniform Resource Locator [URL] encode).	Computer Languages	○	○	○	○	○	○	○	○	○	○	○	○		○	○	○	○	○		
19	Knowledge of cyber defense mitigation techniques and vulnerability assessment tools, including open source tools, and their capabilities.	Computer Network Defense	○	○	○	○	○	○	○	○	○	○	○	○		○	○	○	○	○		
59	Knowledge of Intrusion Detection System (IDS) tools and applications.	Computer Network Defense	○	○	○	○	○	○	○	○	○	○				○	○	○	○	○		
66	Knowledge of intrusion detection methodologies and techniques for detecting host-and network-based intrusions via intrusion detection technologies.	Computer Network Defense	○	○	○	○	○	○	○	○	○	○	○	○		○	○	○	○	○		
146	Knowledge of the types of Intrusion Detection System (IDS) hardware and software.	Computer Network Defense	○	○	○	○	○	○	○	○	○	○				○	○	○	○	○		
153	Skill of identifying capturing, containing, and reporting malware.	Computer Network Defense						○														
181	Skill in detecting host and network based intrusions via intrusion detection technologies (e.g., Snort).	Computer Network Defense	○	○	○	○	○	○	○	○	○	○				○	○	○	○	○		
210	Skill in mimicking threat behaviors.	Computer Network Defense	○	○	○	○	○	○	○	○	○	○	○	○		○	○	○	○	○		
227	Skill in tuning sensors.	Computer Network Defense										○										
252	Knowledge of and experience in Insider Threat investigations, reporting, investigative tools and laws/regulations.	Computer Network Defense																		○		
270	Knowledge of common adversary tactics, techniques, and procedures (TTPs) in assigned area of responsibility (e.g., historical country-specific TTPs,	Computer Network Defense	○	○	○	○	○	○	○	○	○	○	○	○		○	○	○	○	○		
277	Knowledge of defense-in-depth principles and network security architecture.	Computer Network Defense										○						○	○			
353	Skill in collecting data from a variety of cyber defense resources.	Computer Network Defense			○											○	○					
896	Skill in protecting a network against malware.	Computer Network Defense						○	○	○		○										
990	Knowledge of common attack vectors on the network layer.	Computer Network Defense	○	○							○	○						○	○			
991	Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution).	Computer Network Defense	○	○	○	○	○	○	○	○	○	○	○	○		○	○	○	○	○		
992	Knowledge of different operational threat environments (e.g., first generation [script kiddies], second generation [non-nation state sponsored], and third generation [nation state sponsored]).	Computer Network Defense	○	○	○	○	○	○	○	○	○	○	○	○		○	○	○	○	○		
1029	Knowledge of malware analysis concepts and methodology.	Computer Network Defense						○														
1069	Knowledge of general attack stages (e.g., foot printing and scanning, enumeration, gaining access, escalation or privileges, maintaining access, network exploitation, covering tracks).	Computer Network Defense	○	○	○	○	○	○	○	○	○	○	○	○		○	○	○	○			
1087	Skill in deep analysis of captured malicious code (e.g., malware forensics).	Computer Network Defense						○														
1096	Knowledge of malware analysis tools (e.g., Oily Debug, Ida Pro).	Computer Network Defense						○														
1097	Knowledge of virtual machine aware malware, debugger aware malware, and packing.	Computer Network Defense						○														
1098	Skill in analyzing anomalous code as malicious or benign.	Computer Network Defense		○				○				○										
1100	Skill in identifying obfuscation techniques.	Computer Network Defense		○				○				○										
1101	Skill in interpreting results of debugger to ascertain tactics, techniques, and procedures (TTP).	Computer Network Defense						○														
1135	Knowledge of the application firewall concepts and functions (e.g., Single point of authentication/audit/policy enforcement, message scanning for malicious content, data anonymization for PCI and PII compliance, data loss protection scanning, accelerated cryptographic operations, SSL security, REST/JSON processing).	Computer Network Defense									○	○										
163	Skill in conducting information searches.	Computer Skills	○	○	○	○	○	○	○	○	○	○	○	○		○	○	○	○	○		
222	Skill in the basic operation of computers.	Computer Skills	○	○	○	○	○	○	○	○	○	○	○	○		○	○	○	○	○		
235	Skill in using the appropriate tools for repairing software, hardware, and peripheral equipment of a	Computers and Electronics								○												

（注）
「I-5.セキュリティベンダーとの連携」および「I-6.セキュリティ関連団体との連携」は、実態としては各役割の中で実行されるため、その時の役割と同等のスキルとなる。

			リアルタイム基本分析	リアルタイム高度分析	トリアージ情報収集	リアルタイム分析報告	分析内容問合受付	検体解析	リモート対処	オンサイト対処	ネットワークセキュリティ製品基本運用	ネットワークセキュリティ製品高度運用	エンドポイントセキュリティ製品基本運用	エンドポイントセキュリティ製品高度運用	ディープアナリシス（深掘分析）ツール運用	分析基盤基本運用	分析基盤高度運用	既設セキュリティ対応ツール検証	新規セキュリティ対応ツール調査、開発	内部不正検知・防止支援	セキュリティベンダーとの連携	セキュリティ関連団体との連携
264	Knowledge of basic physical computer components and architectures, including the functions of various components and peripherals (e.g., central processing units [CPUs], network interface cards [NICs], data storage).	Computers and Electronics	○	○	○	○	○	○	○	○	○	○	○	○		○	○	○	○	○		
891	Skill in configuring and utilizing hardware-based computer protection components (e.g., hardware firewalls, servers, routers).	Configuration Management							○	○				○								
892	Skill in configuring and utilizing software-based computer protection tools (e.g., software firewalls, anti-virus software, anti-spyware).	Configuration Management							○	○				○								
912	Knowledge of collection management processes, capabilities, and limitations.	Configuration Management													○							
985	Skill in configuring and utilizing network protection components (e.g., firewalls, Virtual Private Networks [VPNs], network Intrusion Detection Systems [IDSs]).	Configuration Management							○	○	○	○	○									
1005	Knowledge of functionality, quality, and security requirements and how these will apply to specific items of supply (i.e., elements and processes).	Contracting/Procurement																	○			
1039	Skill in evaluating the trustworthiness of the supplier and/or product.	Contracting/Procurement																	○			
316	Knowledge of processes for collecting, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of	Criminal Law													○							
982	Knowledge of electronic evidence law.	Criminal Law													○							
983	Knowledge of legal rules of evidence and court procedure.	Criminal Law													○							
25	Knowledge of encryption algorithms (e.g., Internet Protocol Security [IPSEC], Advanced Encryption Standard [AES], Generic Routing Encapsulation [GRE], Internet Key Exchange [IKE], Message Digest Algorithm [MD5], Secure Hash Algorithm [SHA], Triple Data Encryption Standard [3DES]).	Cryptography	○	○	○	○	○	○	○	○	○	○	○	○		○	○	○	○	○		
27	Knowledge of cryptography and cryptographic key management concepts.	Cryptography	○	○	○	○	○	○	○	○	○	○	○	○		○	○	○	○	○		
1114	Knowledge of encryption methodologies.	Cryptography	○	○	○	○	○	○	○	○	○	○	○	○		○	○	○	○	○		
28	Knowledge of data administration and data standardization policies and standards.	Data Management														○	○					
31	Knowledge of data mining and data warehousing principles.	Data Management														○	○					
120	Knowledge of sources, characteristics, and uses of the organization's data assets.	Data Management														○	○					
135	Knowledge of the capabilities and functionality associated with various technologies for organizing and managing information (e.g., databases, bookmarking	Data Management														○	○					
137	Knowledge of the characteristics of physical and virtual data storage media.	Data Management														○	○					
186	Skill in developing data dictionaries.	Data Management															○					
188	Skill in developing data repositories.	Data Management															○					
907	Skill in data mining techniques.	Data Management															○					
910	Knowledge of database theory.	Data Management														○	○					
1007	Skills in data reduction.	Data Management														○	○					
1091	Skill in one way hash functions (e.g., Secure Hash Algorithm [SHA], Message Direct Algorithm [MD5]).	Data Management	○	○	○	○	○	○	○	○	○	○	○	○		○	○	○	○	○		
1120	Ability to interpret and incorporate data from multiple tool sources.	Data Management														○	○					
1126	Knowledge of data classification standards and methodologies based on sensitivity and other risk	Data Management														○	○					
152	Skill in allocating storage capacity in the design of data management systems.	Database Administration														○	○					
178	Skill in designing databases.	Database Administration														○	○					
213	Skill in optimizing database performance.	Database Administration														○	○					
1124	Knowledge of advanced data remediation security features in databases.	Database Administration														○	○					
32	Knowledge of database management systems, query languages, table relationships, and views.	Database Management Systems														○	○					
34	Knowledge of database systems.	Database Management Systems	○	○	○	○	○	○	○	○	○	○	○	○		○	○	○	○	○		
104	Knowledge of query languages such as Structured Query Language (SQL).	Database Management Systems	○	○	○	○	○	○	○	○	○	○	○	○		○	○	○	○	○		
166	Skill in conducting queries and developing algorithms to analyze data structures.	Database Management Systems															○			○		
201	Skill in generating queries and reports.	Database Management Systems				○										○	○			○		
208	Skill in maintaining databases.	Database Management Systems														○	○					
148	Knowledge of Virtual Private Network (VPN) security.	Encryption	○	○	○	○	○	○	○	○	○	○	○	○		○	○	○	○	○		
237	Skill in using Virtual Private Network (VPN) devices and encryption.	Encryption							○		○	○	○			○	○					
917	Knowledge of social dynamics of computer attackers in a global context.	External Awareness	○	○	○	○	○	○	○	○	○	○	○	○		○	○	○	○	○		
15	Knowledge of capabilities and applications of network equipment including hubs, routers, switches, bridges, servers, transmission media, and related hardware.	Hardware								○	○							○	○			
83	Knowledge of network hardware devices and functions.	Hardware								○	○							○	○			
226	Skill in the use of social engineering techniques.	Human Factors	○	○	○	○	○	○	○	○	○	○	○	○		○	○	○	○	○		
8	Knowledge of authentication, authorization, and access control methods.	Identity Management																		○		
79	Knowledge of network access, identity, and access management (e.g., public key infrastructure [PKI]).	Identity Management																		○		
98	Knowledge of policy-based and risk-adaptive access controls.	Identity Management																		○		
191	Skill in developing and applying security system access controls.	Identity Management									○	○	○	○		○	○	○	○	○		
986	Knowledge of organizational information technology (IT) user security policies (e.g., account creation, password rules, access control).	Identity Management																		○		
33	Knowledge of database procedures used for documenting and querying reported incidents.	Incident Management			○	○														○		
37	Knowledge of disaster recovery and continuity of operations plans.	Incident Management									○	○	○	○		○	○					

（注）
「I-5.セキュリティベンダーとの連携」および「I-6.セキュリティ関連団体との連携」は、実態としては各役割の中で実行されるため、その時の役割と同等のスキルとなる。

			リアルタイム基本分析	リアルタイム高度分析	トリアージ情報収集	リアルタイム分析報告	分析内容問合受付	検体解析	リモート対処	オンサイト対処	ネットワークセキュリティ製品基本運用	ネットワークセキュリティ製品高度運用	エンドポイントセキュリティ製品基本運用	エンドポイントセキュリティ製品高度運用	ディープアナリシス（深掘分析）ツール運用	分析基盤基本運用	分析基盤高度運用	既設セキュリティ対応ツール検証	新規セキュリティ対応ツール調査、開発	内部不正検知・防止支援	セキュリティベンダーとの連携	セキュリティ関連団体との連携
60	Knowledge of incident categories, incident responses, and timelines for responses.	Incident Management				○																
61	Knowledge of incident response and handling methodologies.	Incident Management				○			○	○												
216	Skill in recovering failed servers.	Incident Management							○	○												
229	Skill in using incident handling methodologies.	Incident Management							○	○												
978	Knowledge of root cause analysis for incidents.	Incident Management	○	○	○	○																
980	Skill in performing root cause analysis for incidents.	Incident Management		○	○	○																
38	Knowledge of organization's enterprise information security architecture system.	Information Assurance	○	○	○	○	○	○	○	○	○	○	○	○		○	○	○	○	○		
46	Knowledge of fault tolerance.	Information Assurance									○	○	○	○		○	○					
55	Knowledge of information assurance (IA) principles used to manage risks related to the use, processing, storage, and transmission of information or data.	Information Assurance	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○		
183	Skill in determining how a security system should work, including its resilience and dependability capabilities, and how changes in conditions, operations, or the environment will affect these outcomes.	Information Assurance									○	○	○	○		○	○	○	○			
893	Skill in securing network communications.	Information Assurance									○	○						○	○			
895	Skill in recognizing and categorizing types of vulnerabilities and associated attacks.	Information Assurance	○	○	○	○	○	○	○	○	○	○	○	○		○	○	○	○			
49	Knowledge of host and network access control mechanisms (e.g., access control list).	Information Systems/Network							○	○	○	○	○	○				○	○			
58	Knowledge of known vulnerabilities from alerts, advisories, errata, and bulletins.	Information Systems/Network	○	○	○	○	○	○	○	○	○	○	○	○		○	○	○	○			
64	Knowledge of information security systems engineering principles.	Information Systems/Network	○	○	○	○	○	○	○	○	○	○	○	○		○	○	○	○			
70	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	Information Systems/Network Security	○	○	○	○	○	○	○	○	○	○	○	○		○	○	○	○			
77	Knowledge of current industry methods for evaluating, implementing, and disseminating information technology (IT) security assessment, monitoring, detection, and remediation tools and procedures, utilizing standards-based concepts and capabilities.	Information Systems/Network Security																	○			
87	Knowledge of network traffic analysis methods.	Information Systems/Network				○	○	○	○	○	○	○	○	○		○	○	○	○			
138	Knowledge of the Enterprise Network Defense (END) provider reporting structure and processes within one' s own organization.	Information Systems/Network Security				○	○															
150	Knowledge of what constitutes a network attack and the relationship to both threats and vulnerabilities.	Information Systems/Network	○	○	○	○	○	○	○	○	○	○	○	○		○	○	○	○			
175	Skill in developing and deploying signatures.	Information Systems/Network										○										
197	Skill in discerning the protection needs (i.e., security controls) of information systems and networks.	Information Systems/Network																	○			
205	Skill in implementing, maintaining, and improving established security practices.	Information Systems/Network																○				
915	Knowledge of front-end collection systems, including network traffic collection, filtering, and selection.	Information Systems/Network									○	○										
923	Knowledge of security event correlation tools.	Information Systems/Network	○	○	○	○										○	○					
1033	Knowledge of basic system administration, network, and operating system hardening techniques.	Information Systems/Network	○	○	○	○	○	○	○	○	○	○	○	○		○	○	○	○			
1072	Knowledge of network security architecture concepts, including topology, protocols, components, and principles (e.g., application of defense-in-depth).	Information Systems/Network Security	○	○	○	○	○	○	○	○	○	○	○	○		○	○	○	○			
1118	Skill in reading and interpreting signatures (e.g., Snort).	Information Systems/Network	○	○							○	○										
1119	Knowledge of signature implementation impact.	Information Systems/Network										○										
106	Knowledge of remote access technology concepts.	Information Technology Architecture							○													
141	Knowledge of the enterprise information technology (IT) architecture.	Information Technology Architecture							○	○												
76	Knowledge of measures or indicators of system performance and availability.	Information Technology Performance Assessment									○	○	○	○		○	○	○	○			
96	Knowledge of performance tuning tools and techniques.	Information Technology Performance Assessment									○	○	○	○		○	○	○	○			
202	Skill in identifying and anticipating server performance, availability, capacity, or configuration problems.	Information Technology Performance Assessment														○	○	○	○			
203	Skill in identifying measures or indicators of system performance and the actions needed to improve or correct performance, relative to the goals of the	Information Technology Performance Assessment									○	○	○	○		○	○	○	○			
211	Skill in monitoring and optimizing server performance.	Information Technology Performance Assessment														○	○	○	○			
12	Knowledge of communication methods, principles, and concepts (e.g., encoding, signaling, multiplexing) that support the network infrastructure.	Infrastructure Design									○	○										
41	Knowledge of organization's Local Area Network (LAN)/Wide Area Network (WAN) pathways.	Infrastructure Design	○	○	○	○	○				○	○										
50	Knowledge of how network services and protocols interact to provide network communications.	Infrastructure Design	○	○	○	○	○	○	○	○	○	○	○	○		○	○	○	○			
72	Knowledge of local area network (LAN) and wide area network (WAN) principles and concepts, including bandwidth management.	Infrastructure Design									○	○						○	○			
81	Knowledge of network protocols (e.g., Transmission Critical Protocol/Internet Protocol [TCP/IP], Dynamic Host Configuration Protocol [DHCP]), and directory services (e.g., Domain Name System [DNS]).	Infrastructure Design	○	○	○	○	○	○	○	○	○	○	○	○		○	○	○	○			
82	Knowledge of network design processes, including security objectives, operational objectives, and	Infrastructure Design									○	○						○	○			
92	Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol and Internet Protocol [TCP/IP], Open System Interconnection	Infrastructure Design	○	○	○	○	○	○	○	○	○	○	○	○		○	○	○	○			
139	Knowledge of common networking protocols (e.g., Transmission Control Protocol and Internet Protocol [TCP/IP]) and services (e.g., web, mail, Domain Name System [DNS]) and how they interact to provide network communications.	Infrastructure Design	○	○	○	○	○	○	○	○	○	○	○	○		○	○	○	○			

（注）
「I-5.セキュリティベンダーとの連携」および「I-6.セキュリティ関連団体との連携」は、実態としては各役割の中で実行されるため、その時の役割と同等のスキルとなる。

			リアルタイム基本分析	リアルタイム高度分析	トリアージ情報収集	リアルタイム分析報告	分析内容問合受付	検体解析	リモート対処	オンサイト対処	ネットワークセキュリティ製品基本運用	ネットワークセキュリティ製品高度運用	エンドポイントセキュリティ製品基本運用	エンドポイントセキュリティ製品高度運用	ディープアナリシス（深掘分析）ツール運用	分析基盤基本運用	分析基盤高度運用	既設セキュリティ対応ツール検証	新規セキュリティ対応ツール調査、開発	内部不正検知・防止支援	セキュリティベンダーとの連携	セキュリティ関連団体との連携
212	Skill in network mapping and recreating network topologies.	Infrastructure Design									○	○										
271	Knowledge of common network tools (e.g., ping, traceroute, nslookup) and interpret the information results.	Infrastructure Design	○	○	○	○	○	○	○	○	○	○	○	○		○	○	○	○			
1059	Knowledge of networking protocols.	Infrastructure Design	○	○	○	○	○	○	○	○	○	○	○	○		○	○	○	○			
1064	Knowledge of Extensible Markup Language (XML) schemas.	Infrastructure Design	○	○	○	○	○	○	○	○	○	○	○	○		○	○	○	○			
1137	Skill in deploying Service Gateway at the network edge as the first point of contact or proxy into enterprise infrastructure handling layer 7 protocols (e.g., web, XML SOAP, REST, or legacy protocols [EDI]).	Infrastructure Design														○	○					
165	Skill in conducting open source research for troubleshooting novel client-level problems (e.g., online development communities, system security blogging sites).	Knowledge Management										○	○									
230	Skill in using knowledge management technologies.	Knowledge Management					○															
377	Skill in tracking and analyzing technical and legal trends that will impact cyber activities.	Legal, Government, and Jurisprudence	○	○	○	○	○	○	○	○	○	○	○	○		○	○	○	○			
75	Knowledge of mathematics, including logarithms, trigonometry, linear algebra, calculus, and statistics.	Mathematical Reasoning															○					
172	Skill in creating and utilizing mathematical or statistical models.	Modeling and Simulation															○					
187	Skill in developing data models.	Modeling and Simulation															○					
157	Skill in applying host/network access controls (e.g., access control list).	Network Management							○	○												
167	Skill in conducting server planning, management, and maintenance.	Network Management														○	○					
171	Skill in correcting physical and technical problems that impact server performance.	Network Management														○	○					
194	Skill in diagnosing connectivity problems.	Network Management									○	○	○	○								
195	Skill in diagnosing failed servers.	Network Management														○	○					
221	Skill in testing and configuring network workstations and peripherals.	Network Management									○	○										
231	Skill in using network management tools to analyze network traffic patterns (e.g., simple network management protocol).	Network Management									○	○										
902	Knowledge of the range of existing networks (e.g., Private Branching Exchange [PBX], Local Area Networks [LANs], Wide Area Networks [WANs], Wireless Fidelity [WI-FI]).	Network Management									○	○										
903	Knowledge of Wireless Fidelity (WI-FI).	Network Management									○	○										
1073	Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools.	Network Management									○	○										
20	Knowledge of complex data structures.	Object Technology															○					
90	Knowledge of operating systems.	Operating Systems						○	○	○			○	○	○							
113	Knowledge of server and client operating systems.	Operating Systems						○	○	○			○	○	○							
286	Knowledge of file extensions (e.g., .dll, .bat, .zip, .pcap, .gzip).	Operating Systems	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○			
287	Knowledge of file system implementations (e.g., New Technology File System [NTFS], File Allocation Table [FAT], File Extension [EXT]).	Operating Systems											○	○	○							
344	Knowledge of virtualization technologies and virtual machine development and maintenance.	Operating Systems													○							
347	Knowledge of Windows command line (e.g., ipconfig, netstat, dir, nbtstat).	Operating Systems	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○			
364	Skill in identifying, modifying, and manipulating applicable system components within Windows, Unix, or Linux (e.g., passwords, user accounts, files).	Operating Systems											○	○	○							
371	Skill in reading, interpreting, writing, modifying, and executing simple scripts (e.g., PERL, Visual Basic Scripting [VBS]) on Windows and Unix systems (e.g., tasks such as parsing large data files, automating manual tasks, fetching/processing remote data).	Operating Systems	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○			
386	Skill in using virtual machines.	Operating Systems	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○			
1008	Knowledge of how to troubleshoot basic systems and identify operating systems-related issues.	Operating Systems	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○			
1063	Knowledge of Unix/Linux operating system structure and internals (e.g., process management, directory structure, installed applications).	Operating Systems	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○			
1117	Skill in utilizing virtual networks for testing.	Operating Systems									○	○										
1121	Knowledge of Windows and Unix ports and services.	Operating Systems	○	○	○	○	○	○	○	○	○	○	○	○		○	○	○	○			
376	Skill in talking to others to convey information effectively.	Oral Communication				○	○		○	○												
300	Knowledge of intelligence reporting principles, policies, procedures, and vehicles, including report formats, reportable criteria (requirements and priorities), dissemination practices, and legal authorities and restrictions.	Organizational Awareness				○	○													○		
1056	Knowledge of operations security.	Public Safety and	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○		
338	Knowledge of the principal methods, procedures, and techniques of gathering information and producing, reporting, and sharing intelligence.	Reasoning			○	○	○															
350	Skill in analyzing memory dumps to extract information.	Reasoning												○								
383	Skill in using scientific rules and methods to solve problems.	Reasoning					○		○	○												
1021	Knowledge of risk threat assessment.	Risk Management				○																
1011	Knowledge of processes for reporting network security related incidents.	Security				○	○															
116	Knowledge of software debugging principles.	Software Development						○							○			○	○			
168	Skill in conducting software debugging.	Software Development						○							○			○	○			
185	Skill in developing applications that can log errors, exceptions, and application faults.	Software Development																	○			
973	Skill in using code analysis tools to eradicate bugs.	Software Development																	○			
1094	Knowledge of debugging procedures and tools.	Software Development						○							○			○	○			
118	Knowledge of software development models (e.g., Waterfall Model, Spiral Model, Agile Model).	Software Engineering																	○			
119	Knowledge of software engineering.	Software Engineering																	○			
170	Skill in configuring and optimizing software.	Software Engineering																	○			
976	Knowledge of software quality assurance process.	Software Engineering																	○			

（注）
「I-5.セキュリティベンダーとの連携」および「I-6.セキュリティ関連団体との連携」は、実態としては各役割の中で実行されるため、その時の役割と同等のスキルとなる。

			リアルタイム基本分析	リアルタイム高度分析	トリアージ情報収集	リアルタイム分析報告	分析内容問合受付	検体解析	リモート対処	オンサイト対処	ネットワークセキュリティ製品基本運用	ネットワークセキュリティ製品高度運用	エンドポイントセキュリティ製品基本運用	エンドポイントセキュリティ製品高度運用	ディープアナリシス（深掘分析）ツール運用	分析基盤基本運用	分析基盤高度運用	既設セキュリティ対応ツール検証	新規セキュリティ対応ツール調査、開発	内部不正検知・防止支援	セキュリティベンダーとの連携	セキュリティ関連団体との連携
1071	Knowledge of secure software deployment methodologies, tools, and practices.	Software Engineering																	○			
174	Skill in creating programs that validate and process multiple inputs, including command line arguments, environmental variables, and input streams.	Software Testing and Evaluation																	○			
974	Ability to tailor code analysis for application-specific concerns.	Software Testing and Evaluation						○														
294	Knowledge of hacking methodologies in Windows or Unix/Linux environment.	Surveillance						○							○							
51	Knowledge of how system components are installed, integrated, and optimized.	Systems Integration													○							
99	Knowledge of principles and methods for integrating server components.	Systems Integration														○	○					
112	Knowledge of server administration and systems engineering theories, concepts, and methods.	Systems Life Cycle									○	○	○	○	○	○	○					
129	Knowledge of system life cycle management principles, including software security and usability.	Systems Life Cycle									○	○	○	○	○	○	○					
142	Knowledge of the operations and processes for diagnosing common or recurring system problems.	Systems Life Cycle									○	○	○	○	○	○	○					
144	Knowledge of the systems engineering process.	Systems Life Cycle									○	○	○	○	○	○	○					
145	Knowledge of the type and frequency of routine maintenance needed to keep equipment functioning properly.	Systems Life Cycle									○	○	○	○	○	○	○					
204	Skill in identifying possible causes of degradation of system performance or availability and initiating actions needed to mitigate this degradation.	Systems Life Cycle									○	○	○	○	○	○	○					
206	Skill in installing computer and server upgrades.	Systems Life Cycle									○	○	○	○	○	○	○					
1061	Knowledge of the life cycle process.	Systems Life Cycle									○	○	○	○	○	○	○					
88	Knowledge of new and emerging Information Technology (IT) and cyber security technologies.	Technology Awareness	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○			
155	Skill in applying and incorporating information technologies into proposed solutions.	Technology Awareness																	○			
244	Ability to determine the validity of technology trend	Technology Awareness																	○			
282	Knowledge of emerging computer-based technology that has potential for exploitation by adversaries.	Technology Awareness	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○		
297	Knowledge of key industry indicators that are useful for identifying technology trends.	Technology Awareness																	○			
321	Knowledge of products and nomenclature of major vendors (e.g., security suites: Trend Micro, Symantec, McAfee, Outpost, Panda, Kaspersky, etc.) and how differences affect exploitation/vulnerabilities.	Technology Awareness																○	○			
952	Knowledge of emerging security issues, risks, and vulnerabilities.	Technology Awareness	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○		
278	Knowledge of different types of network communication (e.g., Local Area Network [LAN], Wide Area Network [WAN], Metropolitan Area Network [MAN], Wireless Local Area Network [WLAN], Wireless Wide Area Network [WWAN]).	Telecommunications									○	○										
3	Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems.	Vulnerabilities Assessment	○	○							○	○										
4	Ability to identify systemic security issues based on the analysis of vulnerability and configuration data.	Vulnerabilities Assessment							○	○												
10	Knowledge of application vulnerabilities.	Vulnerabilities	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○		
93	Knowledge of packet-level analysis.	Vulnerabilities	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○		
95	Knowledge of penetration testing principles, tools, and techniques (e.g., metasploit, neosploit).	Vulnerabilities Assessment	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○		
105	Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).	Vulnerabilities Assessment	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○		
123	Knowledge of system and application security threats and vulnerabilities.	Vulnerabilities Assessment	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○		
214	Skill in performing packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump).	Vulnerabilities Assessment		○		○						○										
225	Skill in the use of penetration testing tools and techniques.	Vulnerabilities Assessment		○		○						○										
233	Skill in using protocol analyzers.	Vulnerabilities		○		○						○										
922	Skill in using network analysis tools to identify vulnerabilities.	Vulnerabilities Assessment		○		○						○										
1062	Knowledge of software reverse engineering techniques.	Vulnerabilities						○														
1089	Knowledge of reverse engineering concepts.	Vulnerabilities						○							○							
1095	Knowledge of how different file types can be used for anomalous behavior.	Vulnerabilities Assessment														○	○					
149	Knowledge of web services, including service oriented architecture, Simple Object Access Protocol (SOAP), and web service description language.	Web Technology	○	○		○					○	○										
900	Knowledge of web filtering technologies.	Web Technology	○	○	○	○	○		○		○	○				○	○	○	○			

免責事項
・本資料の著作権は日本セキュリティオペレーション事業者協議会(以下、ISOG-J)に帰属します。（下記参考文献からの引用部分を除く）
・引用については、著作権法で引用の目的上正当な範囲内で行われることを認めます。引用部分を明確にし、出典が明記されるなどです。
・なお、引用の範囲を超えると思われる場合はISOG-Jへご相談ください(info (at) isog-j.org　まで)。
・本文書に登場する会社名、製品名、サービス名は、一般に各社の登録商標または商標です。本文中では®やTM、©マークは明記していません。
・ISOG-Jならびに執筆関係者は、このガイド文書に関するいかなる責任も負うものではありません。全ては自己責任にてご活用ください。

参考文献
・National Cybersecurity Workforce Framework (NIST)
http://csrc.nist.gov/nice/framework/