

情報セキュリティ知識項目 SecBoK 2021概要

～BoKの原点に戻り、ディクショナリーとして、より多くの方が利用できるよう改訂～

情報セキュリティ知識項目 (SecBoK) 改訂委員会

SecBoK2021説明内容

1. セキュリティ知識分野 (SecBoK) とは
2. SecBoK2021の方向性
3. SecBoK2021の特長
4. グローバル標準との連携

参考: 利用例

1. セキュリティ知識分野(SecBoK)とは

「セキュリティ知識分野(SecBoK)」とは、

JNSA教育部会では、独立行政法人情報処理推進機構(IPA)からの委託事業の実施を契機として、情報セキュリティに関する業務に携わる人材が身につけるべき知識とスキルを体系的に整理した「情報セキュリティスキルマップ」の作成に2003年度から取り組んでいます。2007年からは名称を「セキュリティ知識分野SecBoK (Security Body of Knowledge)」と改め、2016年以降は定期的に改定を行っています。

現行公開版SecBoK2019は、セキュリティ関連業務に従事する人材に求められる1000を超える知識項目の集合になります。多くの方に利用いただけるように、大項目・中項目といった構造化された構成となっており、あわせて下記も提示しています。

- ・想定している「セキュリティ関連業務」の分類(ロール・役割)を提示
- ・各ロールとそれに要求される/会得しているべき知識項目との対応を提示

今回SecBoKは、BoK(Body of Knowledge)の原点に返って、「ディクショナリー的な位置付け」として多くの方に利用いただけることが目的であることを再確認し、「SecBoK2021」として最新の改訂版を公開しました。

2. SecBoK2021の方向性

1. SecBoK (Security Body of Knowledge) の原点に返って

SecBoKは、名前の通り「Body of Knowledge」であるので、ディクショナリー的な位置付けとして多くの方に利用いただけることが目的であることを再確認。

2. ディクショナリーとして、より多くの方が利用できるように

ディクショナリーであるならば、SecBoKを引用していただき、多くの方が使い易い形態にすべきである。多くの方とは、セキュリティ専門人材だけではなく、近年その必要性と人材不足が叫ばれている「プラス・セキュリティ人材」への対応を実現。またジョブチェンジおよび組織異動(事業部門→セキュリティ/IT、セキュリティ/IT→事業部門)される方々も容易に利用できるように改定。

3. Job description (ジョブディスクリプション) の考え方を広め、人材エコシステムの推進に貢献

セキュリティ人材の可視化が様々な方面で進んでいるが、可視化の際のスキル項目として利用いただき、セキュリティ人材不足対応への貢献。

4. グローバル標準との連携で、海外での利用も推進

NIST SP800-181rev.1 (NICE Framework) が、2020年11月にRev1版として改定されたが、SecBoK独自の点は残しつつも、海外での利用も想定し、グローバル標準との連携も進めていく。

3. SecBoK2021の特長

1. カテゴリーの改定で、プラス・セキュリティ人材や大学でも使い易く

今注目されている「プラス・セキュリティ人材」は、ある定義された人材が存在するわけではなく、本来従事している業務にプラスしてセキュリティスキルを身に付けておいてほしい人材のため、業務の種類や立場などによって求められるスキルが異なるが、その中でも共通となるベースのスキルを下記のカテゴリーに集めて、使い易く改定した。

1) まずは、全てのベースとなる「00基礎」「01IT・セキュリティ基礎」「02ITヒューマンスキル」分野のスキルをチェック

まずは、ベースとなるスキルをチェックし易くするため分野カテゴリーを改定

2021ID	旧2019ID	KSA-ID	新旧別	分野	大項目	中項目	レベル	小項目
1	1	K0052	旧NICEに類似項あり	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)
2	2	K0030	旧NICEに類似項あり	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
⋮								
38	991	K0380	新規	01IT・セキュリティ基礎	1ICT	1ICT利活用	L	コラボレーションツールと環境に関する知識
39	992	K0576	新規	01IT・セキュリティ基礎	1ICT	1ICT利活用	L	情報環境に関する知識
⋮								
62	1086	K0239	新規	02ITヒューマンスキル	1コミュニケーション力		L	書面、口頭及び視覚メディアを介して通知する代替方法を含む、メディア制作、コミュニケーション及び普及の手法および方法に関する知識
63	1087	S0070	旧NICEと同一	02ITヒューマンスキル	1コミュニケーション力		L	情報を効率的に伝達するための他者とのコミュニケーションに関するスキル

2) 以降、各自の業務に応じて、セキュリティ専門分野や、ビジネススキルなどをチェックする

3. SecBoK2021の特長

2. Job description(ジョブディスクリプション)の考え方を広め、人材エコシステムの推進役へ

SecBoKのスキル項目を活用して、ジョブディスクリプションに基づく、ジョブ型採用の際にも利用できるような下記職種の例を提示

- ・POC(Point of Contact)

自組織外・自組織内連絡担当、IT部門調整担当

- ・リサーチャー

自組織外・自組織内連絡担当、IT部門調整担当

- ・脆弱性診断士

脆弱性の診断、評価担当

ジョブディスクリプション例① PoC募集

項目	記載例	SecBoKのID ()内は旧ID	NICE(旧版)ID
ロール名	POC		
職務内容 (NCA資料より)	<p><u>自組織外・自組織内連絡担当、IT部門調整担当</u></p> <p>社外窓口として、JPCERT/CC、NISC、警察、監督官庁、NCA、他CSIRT等との連絡窓口となり、情報連携を行う。</p> <p>社内窓口として、IT部門、法務、渉外、広報、各事業部等との連絡窓口となり、情報連携を行う。</p>		
任用前提知識・スキル (SecBoKの対象)	コミュニケーションスキル(相手の意図や感情を理解する)	要追加	—
	情報を効率的に伝達するための他者とのコミュニケーションに関するスキル	63(1087)	S0070
	レポートスキル(難しい内容を、読み手に合わせて書き砕く能力)	65(1089)	なし
追加教育知識・スキル (SecBoKの対象)	ITSSレベル2程度の基礎的なITリテラシー	41(994)	なし
	コミュニケーションスキル(組織として発信する文書の作成スキル)	要追加	—
	メディアリテラシーに相当するスキル(すべての情報をうのみにしてはいけないという批判的視点など)	80(1104)	なし
	セキュリティマネジメントに関する知識	112(81)	K0276
	自社のセキュリティポリシー、規則、実施方法等に関する知識	120(89)	なし
	企業のインシデントレスポンスプログラム、役割及び責任に関する知識	346(315)	K0150
	ボードメンバーを含むすべてのレベルの管理者とのコミュニケーションを行うスキル(例:対人関係スキル、アプローチ力、効果的なリスニングスキル、視聴者のためのスタイルと言語の適切な使用など)	75(1099)	S0356
必要な経験・資格 (参考)	脆弱性情報の発信源(例:アラート、アドバイザリ、正誤表、報告書)に関する知識	209(178)	K0040
	情報収集ならびに情報を生成、報告及び共有するための主要な方法、手順及び技術に関する知識	879(1055)	K0315
あると望ましい経験・資格(参考)	<p>経験: 広報・渉外等部署での業務経験</p> <p>資格: 情報セキュリティマネジメント試験</p>		

ジョブディスクリプション例② リサーチャー募集

項目	記載例	SecBoKのID	NICE(旧版)ID
ロール名	リサーチャー		
職務内容 (NCA資料より)	情報収集担当 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。 単独機器の分析は行うが、相関的な分析はしない。		
任用前提知識・スキル (SecBoKの対象)	英語で書かれた文書を素早く読解する能力	67(1091)	なし
	英語で書かれた文書を正確に読解する能力	68(1092)	なし
	基本的なサイバーセキュリティの概念、原則、制限及び効果に関する知識	49(42)	K0435
	情報検索の実施に関するスキル	29(29)	S0011
追加教育知識・スキル (SecBoKの対象)	メディアリテラシーに相当するスキル(すべての情報をうのみにしてはいけないという批判的視点など)	80(1104)	なし
	レポートスキル(難しい内容を、読み手に合わせて書き砕く能力)	65(1089)	なし
	脆弱性情報の発信源(例:アラート、アドバイザリ、正誤表、報告書)に関する知識	209(178)	K0040
	各メディアの特性に関する知識(情報発信の素早さ、正確さ、スタンス、信ぴょう性など)	434(403)	なし
	チャット/パディリスト、新興の技術、VOIP、IP経由のメディア、VPN、VSAT/ワイヤレス、ウェブメール、クッキーのためのコレクション検索/分析技術及びツールに関する知識	644(613)	K0388
	国家間の関係に関する知識(歴史、政治、地理、経済、軍事、文化、宗教など)	435(404)	なし
	エラー、例外、アプリケーションの障害を記録できるアプリケーションとロギングに関する知識	258(237)	K0229
	サイバー環境の脅威と脆弱性に関する知識	376(345)	K0005
必要な経験・資格 (参考)	経験: 英文のウェブサイトや文献を機械翻訳に頼らずに読解した経験		
	資格: なし		
あると望ましい経験・資格(参考)	経験: ネットワークログやアクセスログの分析経験 資格: CEH(Certified Ethical Hacker)、認定ネットワークディフェンダー(CND)		

ジョブディスクリプション例 ③脆弱性診断士募集

項目	記載例	SecBoKのID	NICE(旧版)ID
ロール名	脆弱性診断士		
職務内容 (NCA資料より)	脆弱性の診断、評価担当 OS、ネットワーク、ミドルウェア、アプリケーションが安全かどうかの検査を行い、診断結果の評価を行う。		
任用前提知識・スキル (SecBoKの対象)	ITSSレベル2程度の基礎的なITリテラシー	41(994)	なし
	脆弱性診断に関する基礎知識	208(177)	なし
	パケットレベル解析に関する知識	193(162)	K0062
	ペネトレーションテストの原理、ツール及び技術に関する知識	210(179)	K0342
	ネットワーク層における一般的な攻撃手法に関する知識	385(354)	K0160
追加教育知識・スキル (SecBoKの対象)	レポーティングスキル(難しい内容を、読み手に合わせて書き砕く能力)	65(1089)	なし
	コミュニケーションスキル(わかりやすくプレゼンテーションできる)	要追加	—
	評価結果と検出事項を含む最終的なセキュリティ評価報告書を作成する能力	166(135)	A0156
	組織のLAN/WANの接続に関する知識	926(808)	K0029
	現在及び新興のサイバーセキュリティ技術に関する知識	48(41)	K0335
	現在及び新興の脅威/攻撃手法に関する知識	384(353)	K0151
	脆弱性情報の発信源(例:アラート、アドバイザリ、正誤表、報告書)に関する知識	209(178)	K0040
サイバー防衛と脆弱性評価ツール及びその能力に関する知識	213(182)	K0013	
必要な経験・資格 (参考)	経験: ユーザー側でのIT利用経験 資格: なし		
あると望ましい経験・資格(参考)	経験: セキュリティツールの利用経験 資格: SecuriST/認定脆弱性診断士		

4. グローバル標準との連携

NIST SP800-181rev.1 (NICE Framework)

- 正式名：Workforce Framework for Cybersecurity
- 組織のサイバーセキュリティ業務を記述するための『共通言語』として、業務と学習者に求められるものを定義
- 2017年に公表したものの改訂版(2020年11月16日)
 - 公的機関と民間の双方のニーズに応えるために柔軟性を向上
 - 「コンピテンシー」(=日本で一般で受け入れられている「行動特性」的な意味ではなく、組織で求められる能力的な概念)を導入
 - スキルの構造要素を「知識(K)」「スキル(S)」「能力(A)」の組合せから、「知識(K)」「スキル(S)」のみの構造に見直し
 - サイバーセキュリティ分野の変化に対応
 - 変化に迅速に対応できるよう、フレームワーク本体から、知識・スキル・コンピテンシー・ロール等のリストを分離(SP800-181本体は12ページ)
 - 分離したリストの更新版については2021年以降に公表予定

SecBoKでは、分離したリストの更新が公開された後、連携の方向を検討予定

参考:各ロールとの適合度の例(1)

セレクト知識分 ((S) BoK) ノースキルマップ 19年版 全社 - 表

※特定事業活動関係人日本ネットワークセキュリティ協会 教育課 情報セキュリティ知識項目 (SecBoK) 教育委員会作成 SecBoK2019参考

<ロール毎の必須知識・スキル>

1	習得スキル (教育課程で習得して頂くべき知識・スキル)
2	必須スキル (教育課程の修得に際して必要となる知識・スキル)
0.5	参考スキル (教育課程に際して必要ではないが、あるとよい知識・スキル)

※「習得スキル」と「必須スキル」の異同
習得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こと、当該教育を受けたこととなる人材となる

<知識・スキルのレベル>

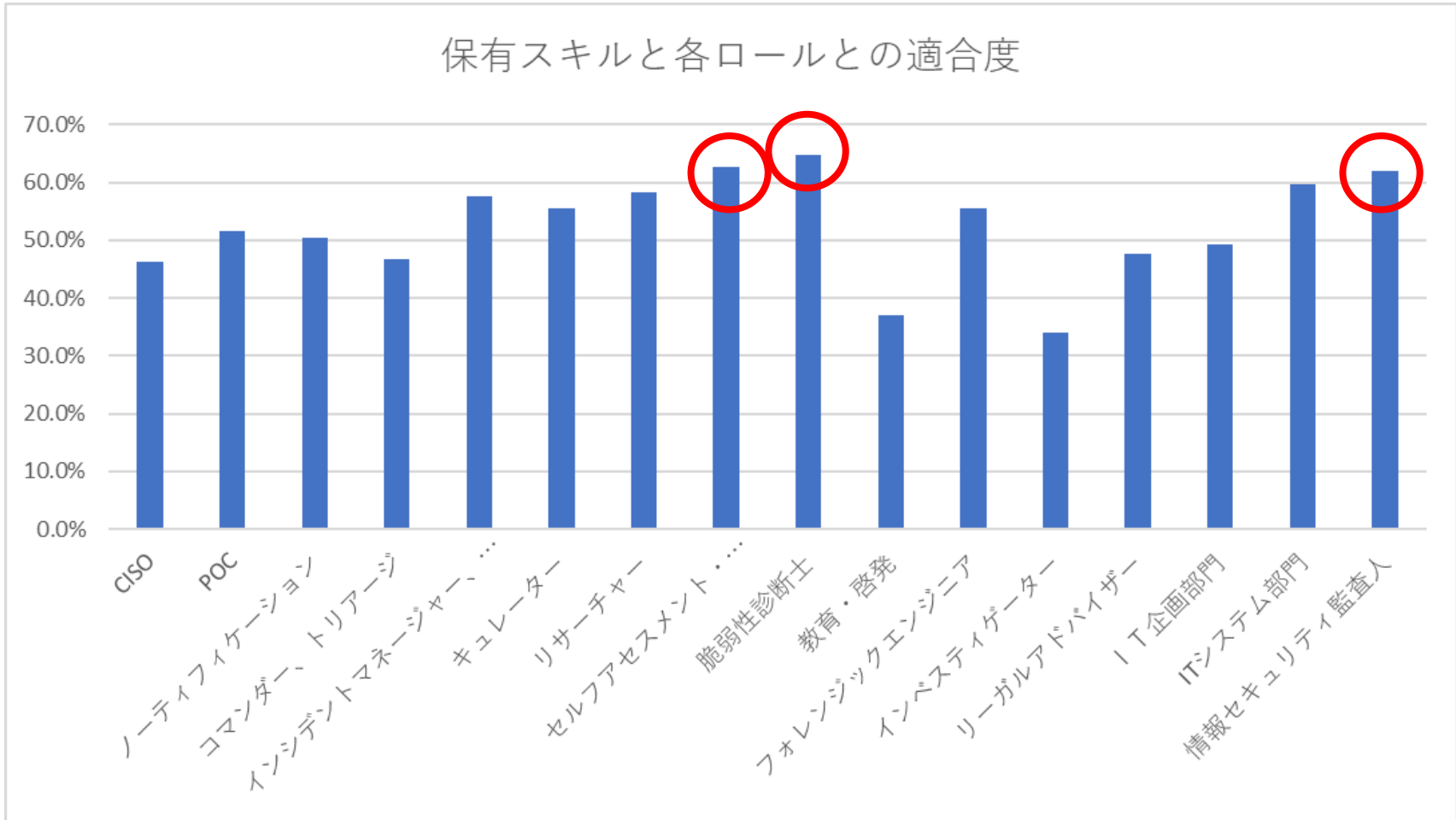
L	低 (初級程度) 3年未満での修得可能
M	中 (初級) 3年以上おおよそ3年未満の修得可能
H	高 (中級) 3年以上おおよそ5年以上の修得可能
P	エキスパート (情報技術、インフラの専門家) に関するもの、今回はレベル分けの對象外

KSA ID	新旧標	IBRD	分野	大項目	中項目	レベル	小項目	保有スキル	各ロールとの適合度																			
									CSO	POC	アネキニク	コンテ	インフラ	クラウド	リテラ	セキュリティ	経営	コンプライアンス	インフラ	セキュリティ	IT	セキュリティ						
1	K0052	INCEI3C	75	00基礎	1数値情報学	L	数字に関する知識 (例: 割合、三角法、線形代数、微積分、統計、操作)	●																				
2	K0030	INCEI3C	42	00基礎	2計算機・通信工	L	コンピュータ・ネットワーク (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	INCEI3C	32	00基礎	2計算機・通信工	L	マンマシンインタラクションの原理に関する知識																					
4	K0055	INCEI3C	78	00基礎	2計算機・通信工	L	マイクロプロセッサに関する知識																					
5	K0061	INCEI3C	92	00基礎	2計算機・通信工	L	ネットワーク上でドライバがどのように運ばれるか (例: TCP/IP、OSI、MTL 実行) に関する知識	●	2	1		1	1	1	1												1	
6	K0108	INCEI3C	281	00基礎	2計算機・通信工	L	各種タイプの基本構成、用途及び種々の範囲での適用に関する知識 (コンピュータと関連のネットワーク、衛星、ファイバ、無線)	●																			1	
7	K0109	INCEI3C	284	00基礎	2計算機・通信工	L	多様な構成要素と周辺機器の機能を含め、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) の機能を含め、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	●																				
8	K0113	INCEI3C	278	00基礎	2計算機・通信工	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	INCEI3C	281	00基礎	2計算機・通信工	L	電子デバイスに関する知識 (例: コンピュータシステム/コンピュータ、アクセス制御デバイス、デジタルカメラ、デジタルシミュレータ、電子オーガナイゼーション、ハードドライブ、メモリカード、モジュール、ネットワークインターフェース、ネットワークアダプタ、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)	●																				0.5
10	K0138	INCEI3C	900	00基礎	2計算機・通信工	L	WiFiに関する知識	●																				1
11	K0395	INCEI3C	22	00基礎	2計算機・通信工	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構成/コンピュータネットワーク、ネットワークの種類など)	●																				1
12	K0491	新標	-	00基礎	2計算機・通信工	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、アドレスリング、ネットワークアーキテクチャ/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
13	K0516	新標	-	00基礎	2計算機・通信工	L	ハブ、スイッチ、ルータ、ファイアウォールなどを含め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
14	K0555	新標	-	00基礎	2計算機・通信工	L	TCP/IP ネットワーキングプロトコルに関する知識	●																				1
15	K0598	新標	-	00基礎	2計算機・通信工	L	通信の基礎に関する知識	●																				1
1141	A0171	新標	-	15関連領域	3教育	M	訓練と教育の必要性に関する評価を行う能力																					1
1142	A0042	新標	-	15関連領域	3教育	M	キャリアパスの機会を開発する能力																					
1143	A0053	新標	-	15関連領域	3教育	M	人材のトレンドデータの有効性を判断する能力																					
1144	S0128	新標	-	15関連領域	3教育	L	人材および人材システムの使用に関するスキル																					
1145	A0022	新標	-	15関連領域	3教育	M	社会人教育の原則を適用する能力																					

「保有スキル」列に、自身の保有しているスキルに●を入力すると、各ロールに対応するポイントが算出される。その結果のロール別対応ポイントを棒グラフ化した例が次ページになる。

Total Point	183.3	74.3	95.0	174.3	224.3	220.0	200.3	240.0	207.3	89.0	215.3	78.3	91.3	119.0	244.0	178.0
SecBoK基準	183.3	74.3	95.0	174.3	225.0	220.0	200.3	240.0	207.3	89.0	215.3	78.3	91.3	119.0	244.0	178.0
SecBoK全1ポイントへ換算	132.0	39.0	77.0	183.0	210.0	210.0	192.0	214.0	207.0	81.0	187.0	88.0	83.0	112.0	251.0	154.0
●保有資格各ロール対応ポイント	75.3	38.3	48.0	81.3	129.3	122.0	117.0	150.3	134.3	33.0	119.3	28.0	43.3	58.3	145.3	109.0
保有資格各ロールの割合	48.2%	51.7%	50.3%	48.7%	57.8%	55.2%	58.4%	62.7%	64.8%	37.1%	55.3%	34.0%	47.3%	49.2%	59.8%	61.9%

参考：各ロールとの適合度の例（2）



この例では、この人材は脆弱性診断士に求められるスキルに適合しており、セルフアセスメントや情報セキュリティ監査人が続いていることがわかる。

参考：大学シラバスとの連携例(1)

各授業とSecBoK項目とのマッピング

大学各授業

*J17とは、世界標準である米国IEEE/ACMのCC2001-CC2005を土台として、日本の情報専門教育の状況に対応した見直しを行い、まとめたカリキュラム標準。

<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)
 - 0.5** 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)

2021ID	ID 2019ID	KSA-ID	新旧別	分野	大項目	中項目	レベル	小項目	情報数学	コンピュータアーキテクチャ	データベース	コンピュータネットワーク	情報セキュリティ概論	オペレーティングシステム	プログラミング演習基礎	認証とアクセス制御	Web構築	ネットワークセキュリティ	コンピュータビジョン	インテリジェント	リスクマネジメント	セキュリティマネジメント	著作権・プライバシー保護	プロジェクマネージメント	
1	1	K0052	IBNICEに類似項あり	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)	●																
2	2	K0030	IBNICEに類似項あり	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	3	K0036	IBNICEと同一	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		●			●												
4	4	K0055	IBNICEと同一	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	5	K0061	IBNICEとほぼ同一	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				●													
6	6	K0108	IBNICEに類似項あり	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適用に関する知識(コンピュータと電話のネットワーク、衛星、ファイバ、無線)																	
7	7	K0109	IBNICEに類似項あり	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、テラストレージ)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		●															
8	8	K0113	IBNICEとほぼ同一	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)				●													
9	9	K0114	IBNICEとほぼ同一	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)																	
10	10	K0138	IBNICEに類似項あり	00基礎	2計算機・通信工学		L	Wi-Fiに関する知識				●													
11	11	K0395	IBNICEとほぼ同一	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)				●													
12	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)				●													
13	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				●													
14	14	K0555	新規	00基礎	2計算機・通信工学		L	TCP/IPネットワークングプロトコルに関する知識				●													
15	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				●													

この例では、赤枠内は大学の各授業である。その授業内で学べる内容をSecBoKスキル項目とマッピングしている。これによりシラバス作成の際にも、各授業で学べるスキルを明確にすることができる。またSecBoKは、情報系大学のカリキュラム標準である「情報セキュリティ(J17-CyberSecurity)」と連携しているためカリキュラム標準に沿ったシラバス作成が可能となる。

参考：大学シラバスとの連携例(2) 各授業とSecBoK役割(ロール)とのマッピング

大学各授業	SecBoK役割																
	CISO	COO	ノーテックイシュー	コンダクター	インシデントレスポンス	インシデントハンディ	セキュリティー	リサーチャー	セルフアセスメント	脆弱性診断士	教育・啓発	フォレンジック	インベスティガター	リーガルアドバイザー	IT企画部門	ITシステム部門	情報セキュリティ監査人
情報数学	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
コンピュータアーキテクチャ				●	●	●	●	●	●	●	●	●	●	●	●	●	
データベース論					●	●	●	●	●	●	●	●	●			●	
コンピュータネットワーク				●	●	●	●	●	●	●	●	●	●		●	●	
情報セキュリティ概論	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
オペレーティングシステム				●	●	●	●	●	●	●	●	●	●		●	●	●
プログラミン演習基礎					●	●	●	●	●	●	●	●	●			●	
認証とアクセス制御				●	●	●	●	●	●	●		●	●		●	●	
Web構築																●	
ネットワークセキュリティ				●	●	●	●	●	●	●		●	●			●	
コンピュータフォレンジック												●					
インシデント対応	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
リスクマネジメント	●	●	●	●	●	●	●	●	●	●	●	●	●		●	●	
セキュリティマネジメント	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
著作権・プライバシー保護														●			●
プロジェクトマネジメント	●			●	●										●	●	

この例では、赤枠内は大学の各授業である。その授業内で学べる内容とSecBoK各役割(ロール)とマッピングしている(青枠)。これにより、授業内容作成の際に、どんな人材育成を目標にしているかを明確にすることができる。また、学生側も自身の目指す人材像を意識して必要なスキルを学べる授業の履修を選択することが可能となる。

JNSA