NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

「SecBoK2021解説」

BoKの原点に返り、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定された最新版を解説

教育部会 部会長
iU情報経営イノベーション専門職大学 教授
平山 敏弘

本日の概要

セキュリティ知識分野（SecBoK）人材スキルマップ2021年版」は、2016年4月の大規模改定以降、ITベンダー・セキュリティベンダーのみならず、多くの企業においてセキュリティ人材育成の際の参考資料として活用されてきました。また教育界との連携も深めてきました。しかし、逆に多くの場面でSecBoKを利用いただきたいとの思いから、SecBoK側が様々な分野への適用を意識する傾向もありました。そこでSecBoK2021では、BoK（Body of Knowledge）であるとの原点に立ち返り、ディクショナリー（辞書）的位置付けとして、より多くの方が参照できることを目標にするとともに、近年その必要性が叫ばれている「プラス・セキュリティ人材」にも適用できる様に改定をおこないました。

当セッションでは、最新版であるSecBoK2021の特長について、作成者自らが解説させて頂くとともに、産学における使用例についてもお話させて頂きます。

SecBoK2021説明内容

1. セキュリティ知識分野（SecBoK）とは

2. セキュリティ人材育成　最近の傾向

3. SecBoK2021の特長

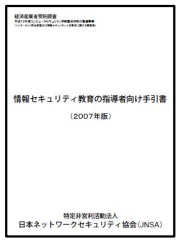
4. SecBoK2021活用例

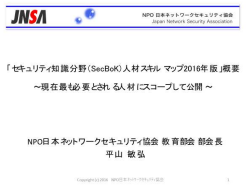
1.セキュリティ知識分野（SecBoK）とは

1.1 セキュリティ知識分野（SecBoK）経緯

「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。





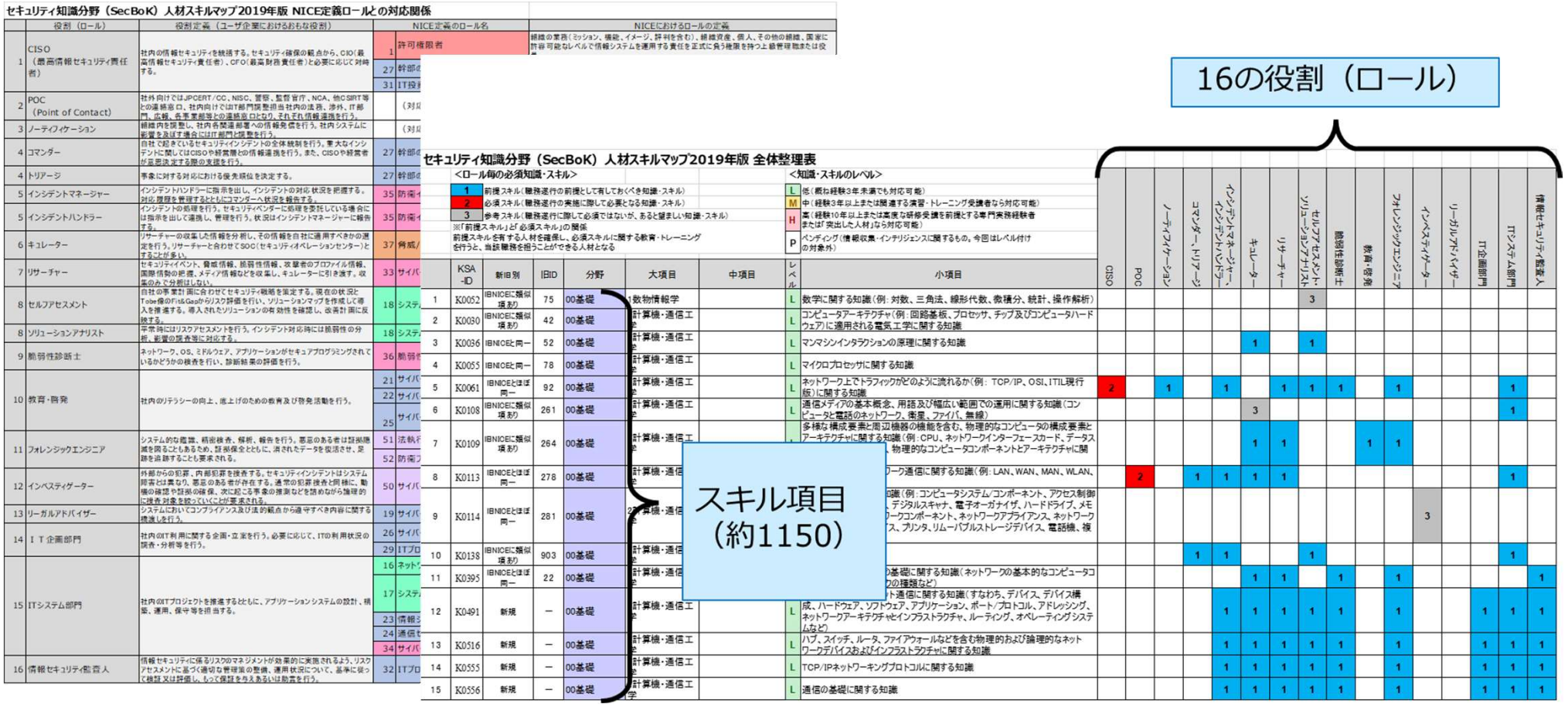
【SecBoK改定経緯】

1） IPAからの依頼で、2004年/2005年に、情報セキュリティスキルマップを作成
2） JNSAよりSecBoKとして名称変更し、経済産業省受託事業のアウトプットとして公開
「情報セキュリティ教育の指導者向け手引書（2007年版）」知識分野がSecBoKの基に
3） ISEPA より、「情報セキュリティ人財アーキテクチャガイドブック」を公開
「セキュリティ知識分野（SecBoK）」として公開
4） SecBokを参考に、2009年に「情報セキュリティプロフェッショナル教科書」出版
5） NIST NICEフレームワークを参考に大規模改定をおこない、SecBoK2016を公開

1.2 SecBoKの役割と知識項目

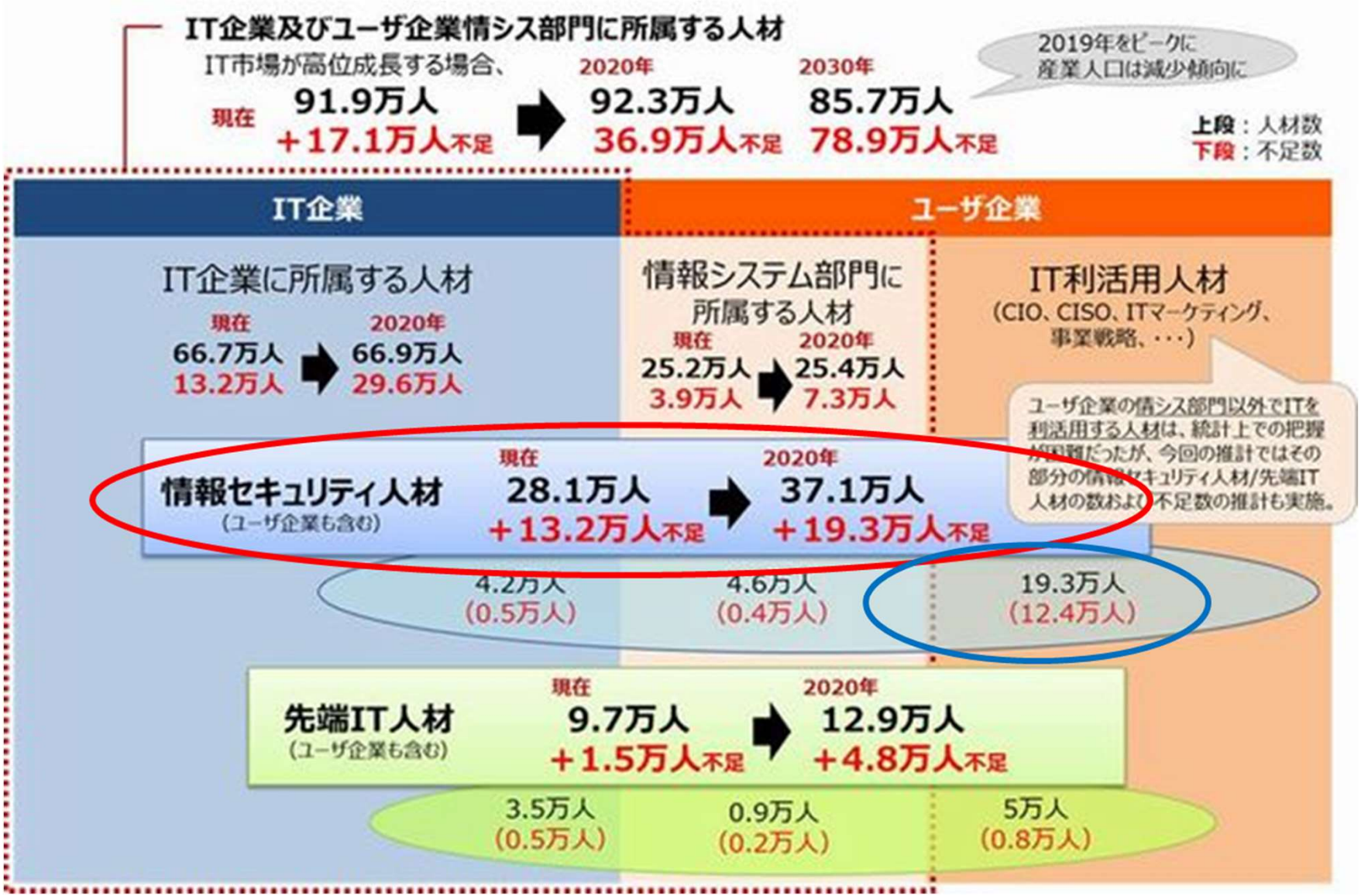
「セキュリティ知識分野（SecBoK）」とは、

・想定している「セキュリティ関連業務」の16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



2.セキュリティ人材育成
最近の傾向

2.1 本当に足りない人材は？ ここの数値に注目



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

2.2 ユーザ企業でのセキュリティ人材不足が問題

約8万人の業種別内訳

業種	（人） 不足数
農林業・水産業・鉱業	256
建設・土木・工業	2,764
電子部品・デバイス・電子回路製造業	1,403
情報通信機械器具製造業	605
電気機械器具製造業	1,150
その他製造業	15,853
電気・ガス・熱供給・水道業	81
通信業	683
情報サービス業	1,885
その他の情報通信業	1,717
運輸・郵便業	6,719
卸売業・小売業	14,480
金融業・保険業	4,957
不動産業・物品賃貸業	1,547
学術研究・専門技術者	1,014
宿泊業・飲食サービス業	3,535
生活関連サービス業・娯楽業	3,301
教育・学習支援業	2,084
医療・福祉	8,473
複合サービス業	614
その他サービス業	8,462
計	81,590

特に情報関連以外の

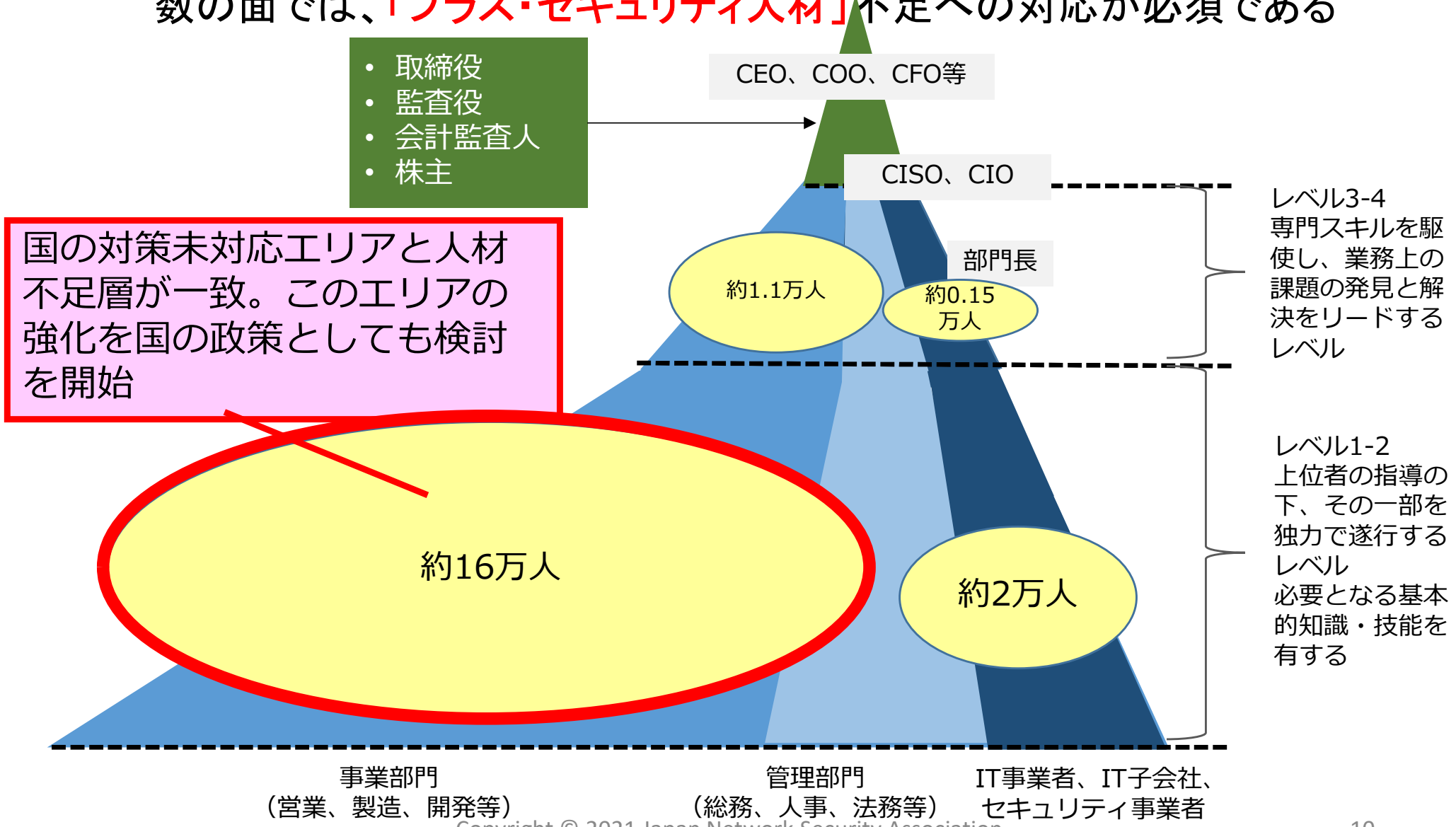
・製造業
・卸売業・小売業
・医療・福祉

などのユーザ業種における人材不足が顕著

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

2.3 セキュリティ人材不足数をマッピング

数の面では、「プラス・セキュリティ人材」不足への対応が必須である



2.4 育成が必要な「プラス・セキュリティ人材」

「プラス・セキュリティ人材」とは、「本来の業務を担いながら **IT を利活用する中でセキュリティスキルも必要**となる人材であり、人材が大きく不足しているのは、プラス・セキュリティ人材」である。

出典：日本サイバーセキュリティ・イノベーション委員会（JCIC)レポート
「セキュリティ人材不足の真実と今なすべき対策とは」
https://www.j-cic.com/pdf/report/Human-Development-Plus-Security.pdf

IPA公開レポートでは、『ITに関わる業務（IT戦略立案から設計・開発、運用保守など）遂行の中でセキュリティスキルを活用している人が多いが、このような人材は「プラス・セキュリティ人材」と呼ばれ、適切な**サイバーセキュリティ対策実現の要となる人材**であると考えられます。』

出典：独立行政法人 情報処理推進機構（IPA）
「情報処理安全確保支援士(登録セキスペ)の活動に関する実態調査」調査報告書について
https://www.ipa.go.jp/siensi/data/rissresearch.html

IPAレポートを紹介する記事では、『**ITに関する多くの業務の中でセキュリティにも携わって**おり、IPAは、この属性の回答者をセキュリティ対策の要になる「プラス・セキュリティ人材」と命名した。』と報じている。

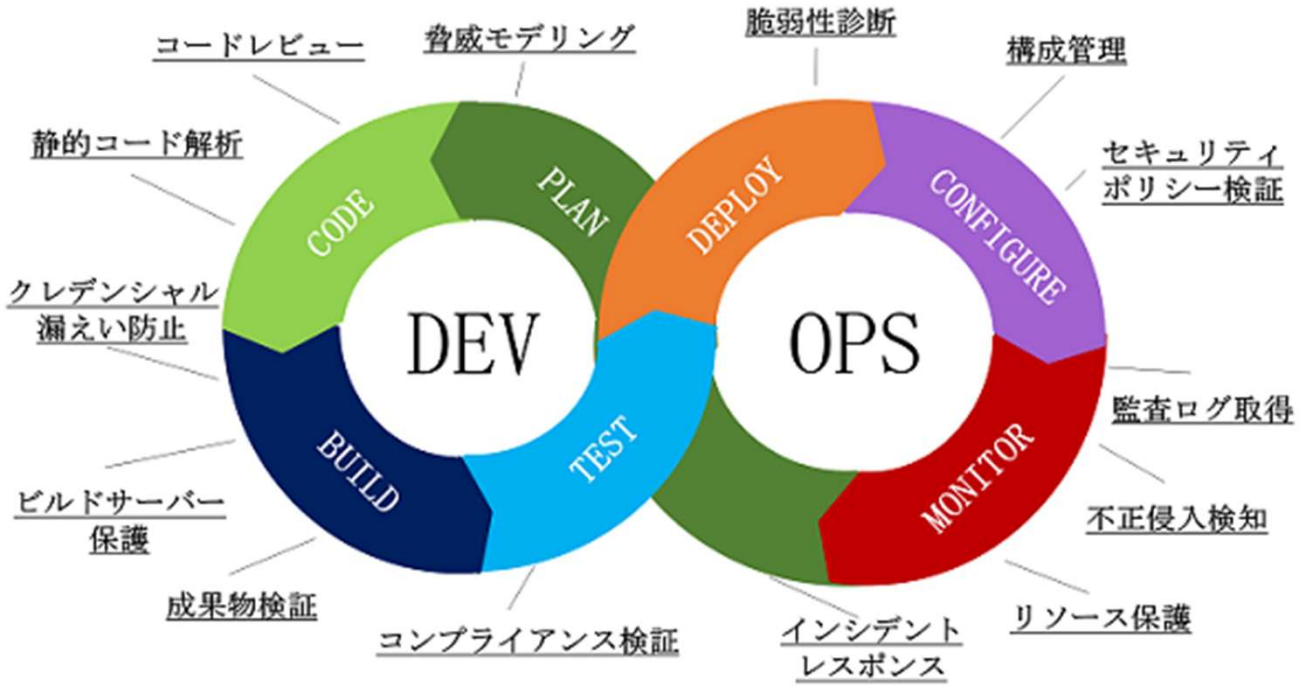
出典：ZDNet Japan記事「セキュリティの国家資格者、6割はセキュリティ業務を担当--IPA調査」
https://japan.zdnet.com/article/35140727/

2.5 DevSecOpsと攻めのプラス・セキュリティ

DevOpsモデルの上で実行される、開発と運用が統合されたライフサイクルでは、あらゆる段階にセキュリティの要素を組み込むべきです。セキュリティを全ての段階に組み込むことで、ビジネス目標達成のためのライフサイクルを迅速かつ安全に実行することが可能になります。

出典：トレンドマイクロ社DevSecOps時代のCloud Security!
https://www.trendmicro.com/ja_jp/business/campaigns/aws/resources/devsecops_whitepaper.html

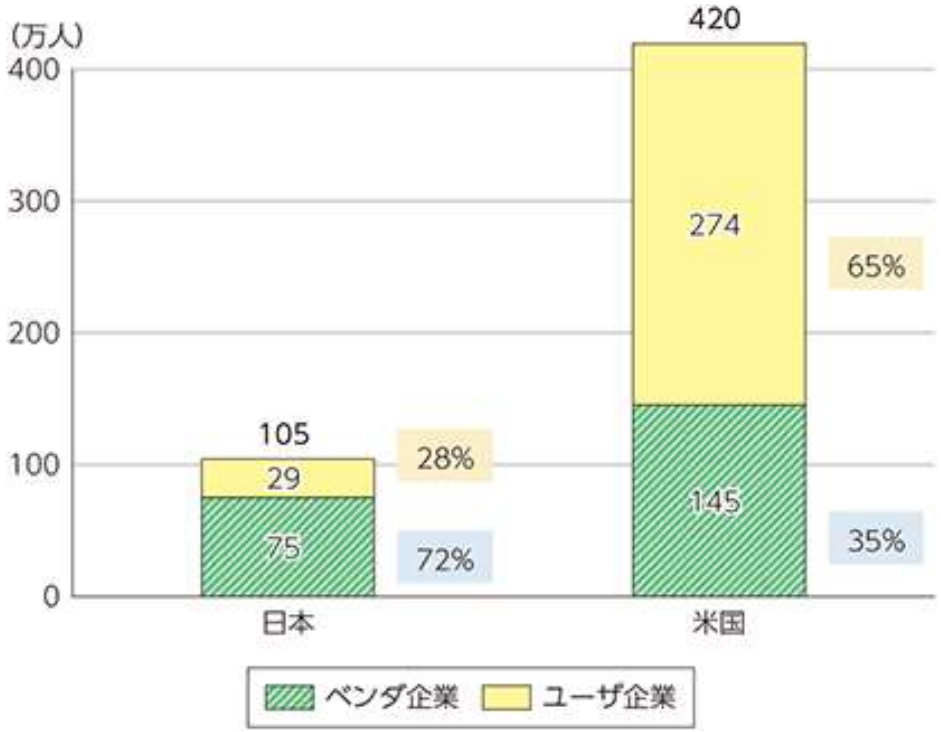
DevSecOps
ライフサイクル



ライフサイクルが短く周期のスピードが速いDevSecOps環境においては、セキュリティ専門家をチームメンバーに置くことは難しく、また外注依存も厳しいケースが多いため、**開発メンバーにプラス・セキュリティのスキル・意識が求められる。**

2.6 ユーザ企業にプラス・セキュリティ人材不足 これではDevSecOpsは無理

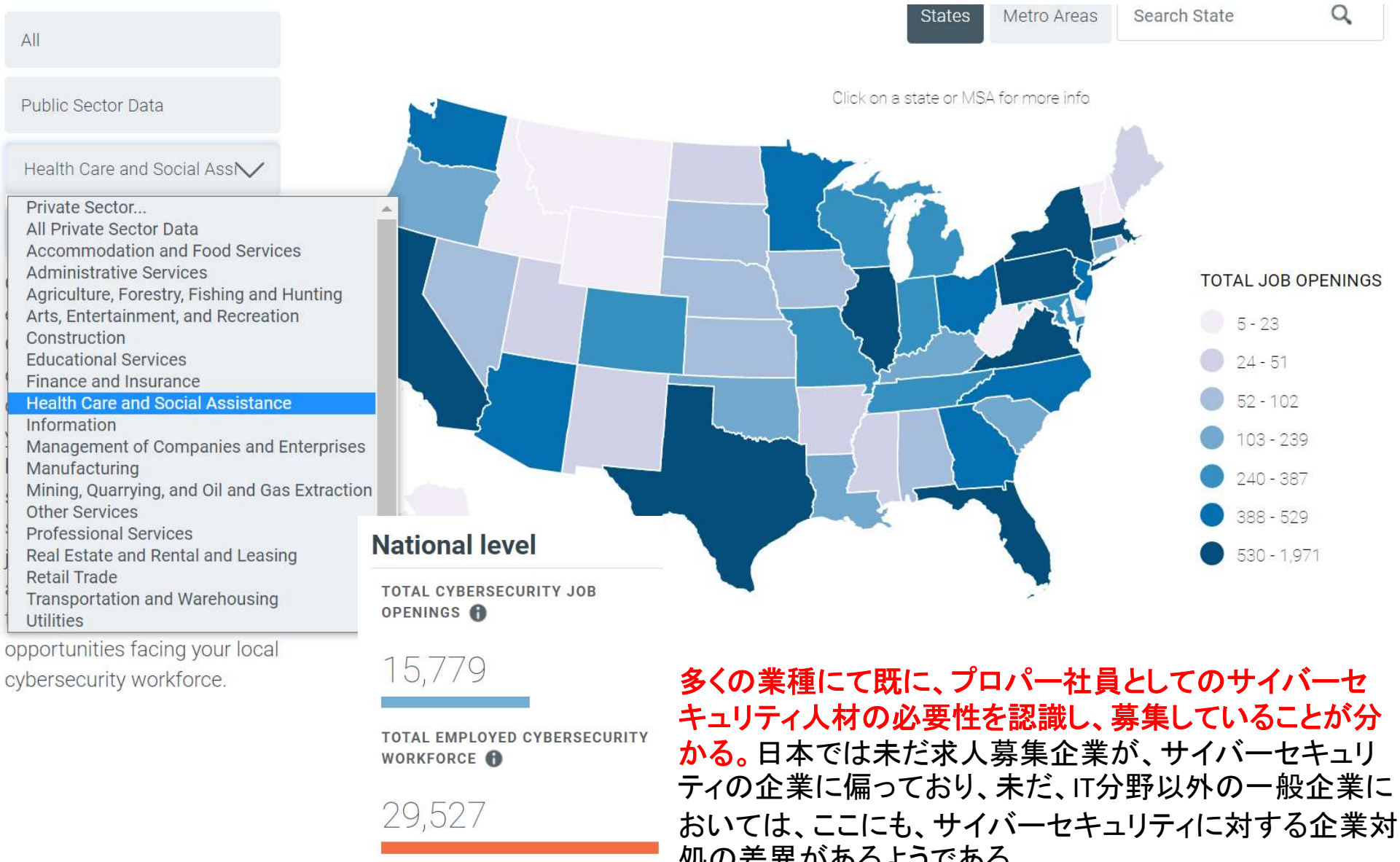
我が国でICT利活用によるイノベーション促進及び付加価値増加を目指すにあたり、現状では、ユーザ企業にICT人材が少ないという構造的問題があることについて補足する。
我が国は米国と比較して、ICT人材の数が少なく、さらに人材がユーザ企業側に少なくベンダ側に偏在している傾向がある。独立行政法人情報処理推進機構の「IT人材白書2017」では、2015年の日米の情報処理・通信に携わる人材数を推計している



日本と米国の情報処理・通信に携わるICT人材
出典：総務省「平成30年版情報通信白書」

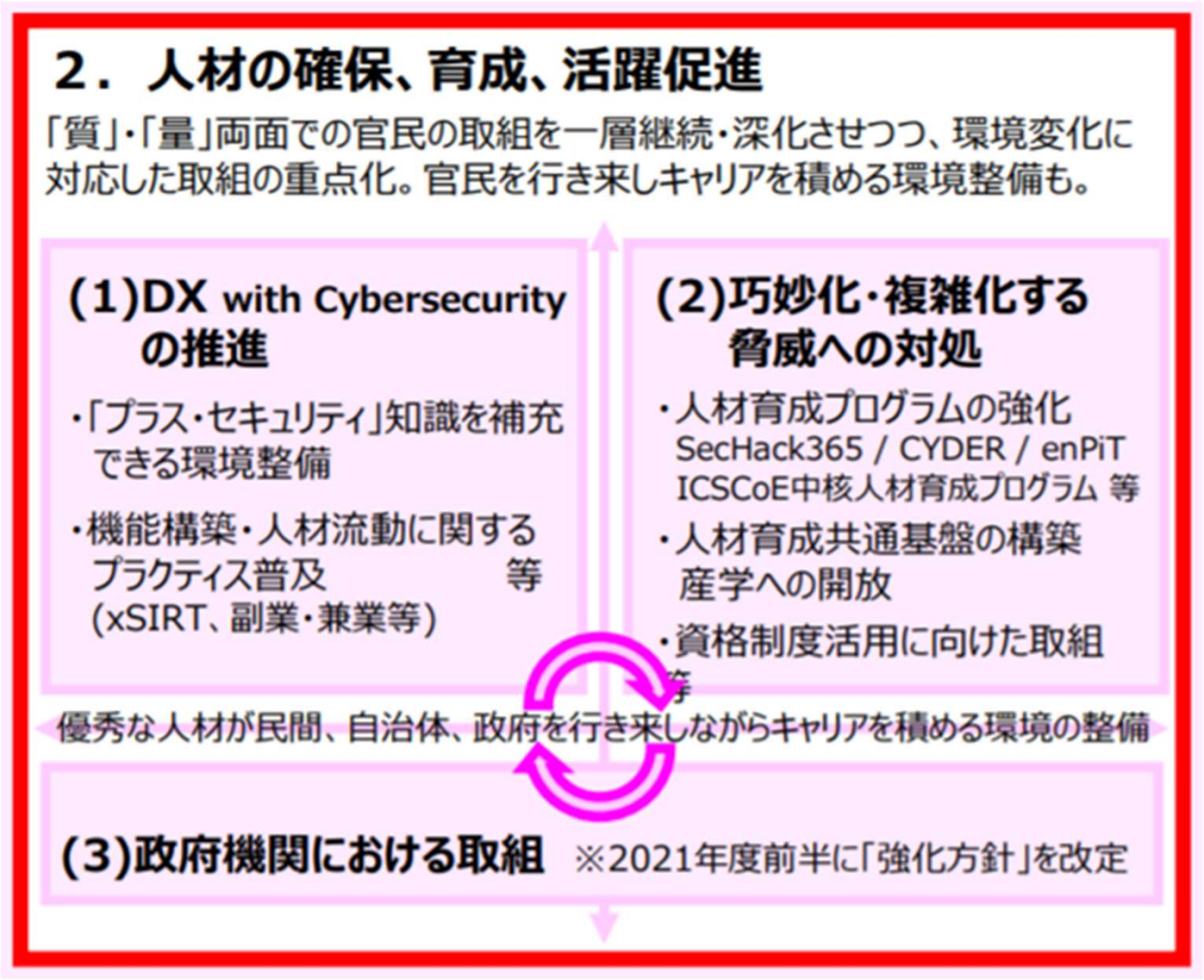
従来から言われていることであるが、日本においては、ユーザ企業にICT人材が少ないという構造的特徴があるが、当然セキュリティ人材も同様であると考えられる。
しかし、**この特徴が、DevOps（DevSecOps）開発を困難なことにしている。**

2.7 ユーザ企業においてのセキュリティ人材募集 米国では当たり前の世界（医療関連でも1.6万人）



多くの業種にて既に、プロパー社員としてのサイバーセキュリティ人材の必要性を認識し、募集していることが分かる。日本では未だ求人募集企業が、サイバーセキュリティの企業に偏っており、未だ、IT分野以外の一般企業においては、ここにも、サイバーセキュリティに対する企業対処の差異があるようである。

2.8 国においても、「プラス・セキュリティ」が検討課題に



NISC（内閣サイバーセキュリティセンター）では、2021年度から始まる、「次期サイバーセキュリティ戦略」において、横断的な施策の1つである「人材確保、育成、活躍促進」で、「プラス・セキュリティ知識を補充できる環境整備」として取り上げている

出典：NISC「次期「サイバーセキュリティ戦略」骨子について（普及啓発・人材育成関係）」

2.9 サイバー議連にも「プラス・セキュリティ」が

令和3年5月、サイバーセキュリティ対策推進議員連盟（会長：野田聖子代議士）が開催され、提言が出されています。

https://www.suzukihayato.jp/post/210525-1

【提言概要】

1．DX with Cybersecurity

経営層から現場まで包括的な意識改革を進めるためにも、政府においては、「DX with Cybersecurity」の旗を振り、普及啓発に全力を尽くすべきである。

2．サプライチェーンセキュリティ

「サプライチェーン・サイバーセキュリティ・コンソーシアム」とも連携し、各地域におけるセキュリティ・コミュニティの形成を積極的に支援すべきである。

3．人材育成

「DX with Cybersecurity」の観点からは、各事業部門のマネジメント層が自らの担当分野に関する知見に加えてセキュリティに関する知識も保有することが求められる。こうした**「プラス・セキュリティ」人材の育成につき、プログラム策定等必要な施策を講じる必要**がある。

3. SecBoK2021の特長

3.1 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、グルーバル標準との連携も進めていく。

3.2 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

3.3 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

3.4 ジョブディスクリプション例①

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）	自組織外・自組織内連絡担当、IT部門調整担当 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。 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。		
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	ー
	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
	ITSSレベル2程度の基礎的なITリテラシー	41(994)	なし
追加教育知識・スキル （SecBoKの対象）	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	ー
	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
	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
必要な経験・資格 （参考）	経験：業務を通じた顧客・取引先・関係機関等との対話・交渉経験 資格：なし		
あると望ましい経験・資格（参考）	経験：広報・渉外等部署での業務経験 資格：情報セキュリティマネジメント試験		

3.5 ジョブディスクリプション例②

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
	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/バディリスト、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
	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
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）		

3.6 ジョブディスクリプション例③

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	ー
	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. SecBoK2021活用例

4.1 各ロールとの適合度の例（1）

セ リ 知識分 (S BoK) ス スキルマップ 19年版 全体 表

特定非営利活動法人 日本ネットワークセキュリティ協会 教育部会 情報セキュリティ知識項目（SecBoK）改訂委員会作成 SecBoK2019参考

＜ロール毎の必須知識・スキル＞

- 1 前提スキル（業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（業務遂行の実施に際して必須となる知識・スキル）
- 0.5 参考スキル（業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、当該業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（経験年数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資格・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資格保有者または「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）

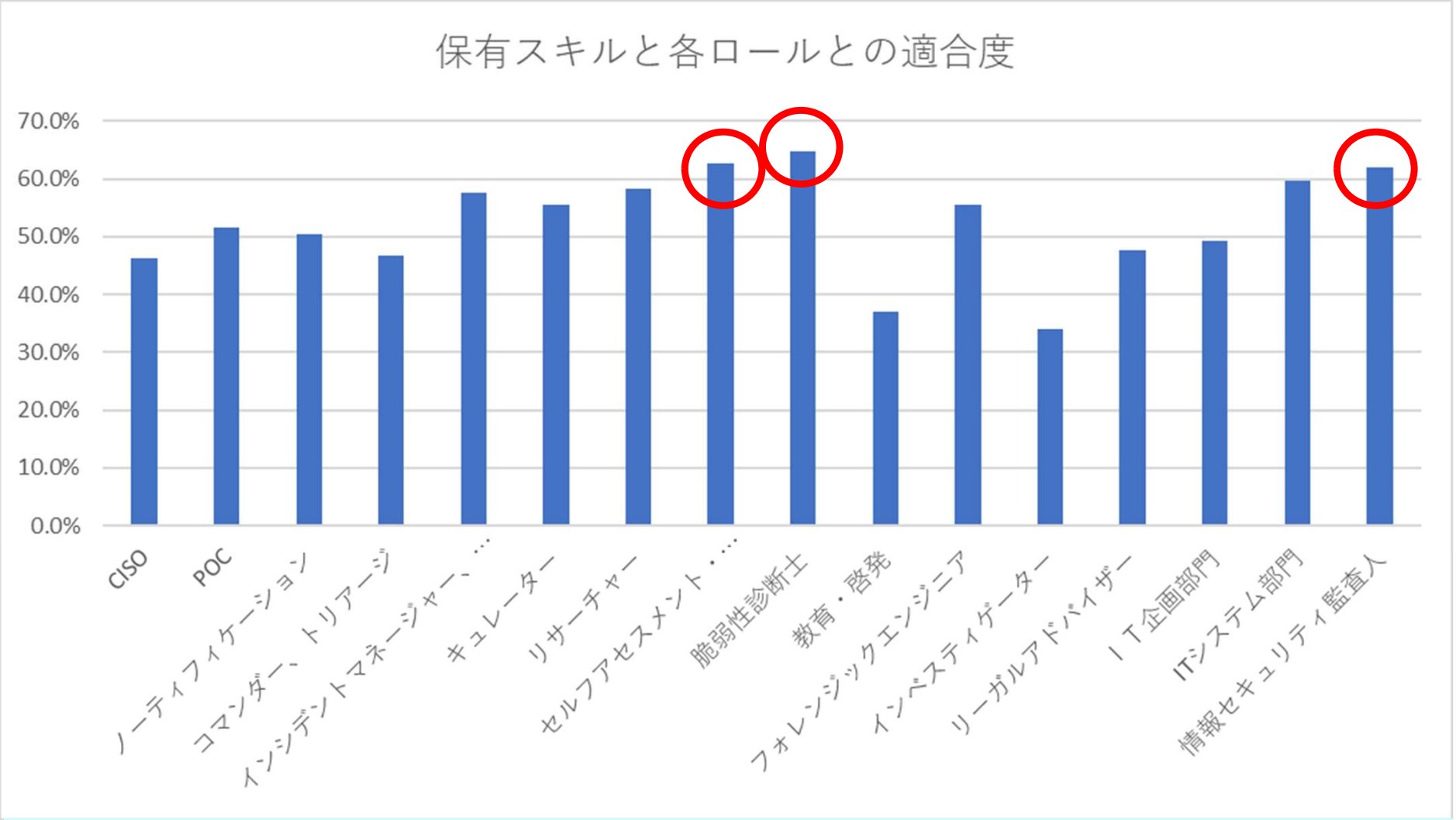
	KSA-ID	新旧項	旧ID	分野	大項目	中項目	レベル	小項目	保有スキル
1	K0052	旧NICEに記載あり	75	00基礎	1数理情報学		L	数学に関する知識（例：対数、三角法、線形代数、微積分、統計、操作解析）	
2	K0030	旧NICEに記載あり	42	00基礎	2計算機・通信工学		L	コンピュータアーキテクチャ（例：回路基板、プロセッサ、チップ及びコンピュータハードウェア）に適用される電気工学に関する知識	●
3	K0036	旧NICEと同一	32	00基礎	2計算機・通信工学		L	マンマシンインタラクションの原理に関する知識	
4	K0055	旧NICEと同一	78	00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翻訳変更	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	●
6	K0108	旧NICEに記載あり	281	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）	●
7	K0109	旧NICEに記載あり	284	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	●
8	K0113	旧NICE翻訳変更	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）	●
9	K0114	旧NICE翻訳変更	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）	●
10	K0138	旧NICEに記載あり	900	00基礎	2計算機・通信工学		L	Wi-Fiに関する知識	●
11	K0395	旧NICE翻訳変更	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）	●
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	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	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	●
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	●
1141	A0171	新規	—	15関連領域	3教育	2評価	M	訓練と教育の必要性に関する評価を行う能力	
1142	A0042	新規	—	15関連領域	3教育	3キャリア	M	キャリアパスの機会を開発する能力	
1143	A0053	新規	—	15関連領域	3教育	3キャリア	M	人材のトレンドデータの有効性を判断する能力	
1144	S0128	新規	—	15関連領域	3教育	9その他	L	人材および人事ITシステムの使用に関するスキル	
1145	A0022	新規	—	15関連領域	3教育	9その他	M	社会人教育の原則を適用する能力	

	CISO	POC	ノーティフィケーション	コマンダー、トリアージ	インシデントマネージャー、インシデントハンドラー	キュレーター	リサーチャー	セルフアセスメント ソリューションアナリスト	脆弱性診断士	教育・啓発	フォレンジックエンジニア	インベスティゲーター	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
1								0.5								
2																
3						1		1								
4																
5	2		1		1		1	1	1		1				1	
6						0.5									1	
7						1	1			1	1					
8		2		1	1	1	1								1	
9												0.5				
10				1	1			1							1	
11						1	1		1		1					1
12					1	1	1	1	1		1			1	1	1
13					1	1	1	1	1		1			1	1	1
14					1	1	1	1	1		1			1	1	1
15					1	1	1	1	1		1			1	1	1
1141										1						
1142																
1143																
1144																
1145																

	CISO	POC	ノーティフィケーション	コマンダー、トリアージ	インシデントマネージャー、インシデントハンドラー	キュレーター	リサーチャー	セルフアセスメント ソリューションアナリスト	脆弱性診断士	教育・啓発	フォレンジックエンジニア	インベスティゲーター	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
Total Point	183.5	74.5	95.0	174.5	224.5	220.0	200.5	240.0	207.5	89.0	215.5	76.5	91.5	119.0	244.0	176.0
SecBoK素点	183.5	74.5	95.0	174.5	223.0	220.0	200.5	240.0	207.5	89.0	215.5	76.5	91.5	119.0	244.0	176.0
SecBoK全1ポイントへ変換	132.0	39.0	77.0	163.0	210.0	210.0	192.0	214.0	207.0	81.0	187.0	69.0	93.0	112.0	231.0	134.0
●保有資格 各ロール対応ポイント	73.5	38.5	48.0	81.5	129.5	122.0	117.0	150.5	134.5	33.0	119.5	26.0	43.5	58.5	145.5	109.0
保有資格と各ロールの適合度	48.2%	51.7%	50.5%	46.7%	57.6%	55.5%	58.4%	62.7%	64.8%	37.1%	55.5%	34.0%	47.5%	49.2%	59.6%	61.9%

「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ます。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。

4.2 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。

4.3 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

JNSA

*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。

大学各授業

<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）
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	旧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	コンピュータフォレンジック	インシデント対応	リスクマネジメン	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
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		●															
3	3	K0036	旧NICE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	旧NICE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	旧NICE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	旧NICE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）																
7	7	K0109	旧NICE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、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		●														
8	8	K0113	旧NICE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	旧NICE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	旧NICE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	旧NICE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ネットワーキ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。

4.4 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

SecBoK役割

大学各授業

授業	CISO	SOC	ノーティフィケーション	コマンダー、トリアージ	インシデントマネージャー、インシデントハンドラー	キュレーター	リサーチャー	セルフアセスメント・ソリューションアナリスト	脆弱性診断士	教育・啓発	フォレンジックエンジニア	インベスティゲーター	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。

SecBoKで、Go to the next stage！

1. セキュリティ人材不足に変化はあるのか？

   求められる人材が**変化している**

2. セキュリティ部門以外にはセキュリティは関係ない

   今後の**企業生き残りをかけたDX化**への対応において、セキュリティは必須

3. ユーザ部門、事業部門で必要なセキュリティ人材とは

   従来の守るためでなく、新たに**お金を稼ぐ視点から「攻めのセキュリティ」**登場。
   DevSecOps開発の実現には、ユーザ・事業部門にもセキュリティ意識を

4. セキュリティ専門知識を活用するためのスキルも必要に

   プラス・セキュリティ人材には、セキュリティ知識の加えて、それを活用するための
   コミュニケーション等の**ヒューマンスキルも必要**

DX with Cybersecurity実現のためにセキュリティ意識の拡大を

様々な分野でSecBoKを活用し、セキュリティ人材育成の加速を！

SecBoK :

Security

Body

of

Knowledge