「DXの推進に不可欠なセキュリティ人材育成」

～教育部会における取組み～

教育部会 部会長
平山 敏弘

本日の要旨

国の標語にもなっている「DX with Cybersecurity」を実現するためには、セキュリティ人材育成が必須となります。

教育部会では、従来の「セキュリティ技術の向上」だけでなく、**「教える経験」**によるセキュリティ専門家の育成を実施しています。また大学や高専および専門学校などへの教育により、**セキュリティの裾野拡大**の活動も長く行なっています。

加えてJNSAから発行している**SecBoK（セキュリティ知識分野）**の利用による海外での人材育成施策の展開なども実績が出ています。

このようなJNSA教育部会独自のセキュリティ人材育成活動のご紹介と、今**必要とされているセキュリティ人材の変化**について、国の施策である「デジタル田園都市国家構想や**DX推進人材**」との関連も含めて、お話させていただきます。

JNSA教育部会のご紹介

JNSA教育部会とは

社会のニーズや時代の変化に適合したセキュリティ人材育成のため、必要とされる知識・技能等の検討を行い、実際に大学や専門学校等で評価実験を行う。

また、情報セキュリティ**教育のコンテンツ**として、講義シラバスや講義資料および**SecBoK**2023年英語版の作成・公開を通じて、教育界・産業界への展開・使用を促進することで、**情報セキュリティ人材の育成に貢献**する。また、ASEANを中心とした海外教育機関との連携によるセキュリティ人材育成への貢献を目指す。

さらに、継続して講師データベースへの登録講師や講師予備軍の若手による講義・勉強会の開催等、教える場の提供を支援することにより、**JNSA**教育部会**メンバーのスキル向上**を目指す。

【部会としての活動】
・SecBoK2023更新
・辻井重男セキュリティ論文賞の運営委員会、および査読委員会

【ワーキンググループ（WG）活動】
・ゲーム教育WG
・情報セキュリティ教育実証WG
・セキュ女WG
・（新設）教育部会産学連携プロジェクト

日本の国際競争力低下の危機

セキュリティ人材育成との関係について

危機的な日本の国際競争力

IMD「世界競争力年鑑」2022年　総合順位

順位	国名	21年からの順位差	順位	国名	21年からの順位差	順位	国名	21年からの順位差
1	デンマーク	△ 2	22	エストニア	△ 4	43	カザフスタン	▲ 8
2	スイス	▲ 1	23	英国	▲ 5	44	インドネシア	▲ 7
3	シンガポール	△ 2	24	サウジアラビア	△ 8	45	チリ	▲ 1
4	スウェーデン	▲ 2	25	イスラエル	△ 2	46	クロアチア	△ 13
5	香港	△ 2	26	チェコ	△ 8	47	ギリシャ	▲ 1
6	オランダ	▲ 2	27	韓国	▲ 4	48	フィリピン	△ 4
7	台湾	△ 1	28	フランス	△ 1	49	スロバキア	△ 1
8	フィンランド	△ 3	29	リトアニア	△ 1	50	ポーランド	▲ 3
9	ノルウェー	▲ 3	30	バーレーン	—	51	ルーマニア	▲ 3
10	米国	△ 0	31	ニュージーランド	▲ 11	52	トルコ	▲ 1
11	アイルランド	△ 2	32	マレーシア	▲ 7	53	ブルガリア	△ 0
12	UAE	▲ 3	33	タイ	▲ 5	54	ペルー	△ 4
13	ルクセンブルク	▲ 1	**34**	**日本**	**▲ 3**	55	メキシコ	△ 0
14	カナダ	△ 0	35	ラトビア	△ 3	56	ヨルダン	▲ 7
15	ドイツ	△ 0	36	スペイン	△ 3	57	コロンビア	▲ 1
16	アイスランド	△ 5	37	インド	△ 6	58	ボツワナ	△ 3
17	中国	▲ 1	38	スロベニア	△ 2	59	ブラジル	▲ 2
18	カタール	▲ 1	39	ハンガリー	△ 3	60	南アフリカ	△ 2
19	オーストラリア	△ 3	40	キプロス	▲ 7	61	モンゴル	▲ 1
20	オーストリア	▲ 1	41	イタリア	△ 0	62	アルゼンチン	△ 1
21	ベルギー	△ 3	42	ポルトガル	▲ 6	63	ベネズエラ	△ 1

注：「21年からの順位差」は2021年版順位からの上昇（△）、下落（▲）幅を示す。

IMD （国際経営開発研究所）が作成する「世界競争力年鑑」の2022年版では、日本は競争力ランキング34位と、前年よりさらに３ランクダウンとなり、4年連続で30位台と下位に留まっており、危機的な状況です。

国際競争力下位の原因は、「人材」と「デジタル」

特に**人材ランキング**においては**41位**と、2019年から4年連続で下落し、前年より順位を2つ落としており、近年は調査対象国の中でも下位に低迷しています。
また**デジタル競争力**ランキングでも**29位**であり、2021年から順位を1つ落とし、2017年の調査以来、過去最低の順位となってしまいました。
この結果より、国際力を高めるためには、**「デジタル」＋「人材」の育成が急務**であることは明確です。

IMD世界デジタル競争力ランキング2022

1. デンマーク	16. 英国
2. 米国	17. 中国
3. スウェーデン	18. オーストリア
4. シンガポール	19. ドイツ
5. スイス	20. エストニア
6. オランダ	21. アイスランド
7. フィンランド	22. フランス
8. 韓国	23. ベルギー
9. 香港	24. アイルランド
10. カナダ	25. リトアニア
11. 台湾	26. カタール
12. ノルウェー	27. ニュージーランド
13. アラブ首長国連邦（UAE）	28. スペイン
14. オーストラリア	29. 日本
15. イスラエル	30. ルクセンブルク

国際競争力向上のために必須の セキュリティ人材育成

またIMDレポート内では、下記のようにデジタル競争力強化のためには、サイバーセキュリティ対策が、最優先課題と指摘しています。

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

「デジタル競争力のある経済では、**サイバーセキュリティ対策が官民の最優先課題である**ことが、2022年IMD世界デジタル競争力ランキングでも明らかになりました。政府や民間企業は、デジタル競争力のある経済の競争を続けたいのであれば、デジタルインフラをサイバー攻撃から保護する必要があります。これは、IMD WCC（World Competitiveness Center）が本日発表した『IMD世界デジタル競争力ランキング（2022年版）』の**主要な発見**です。」

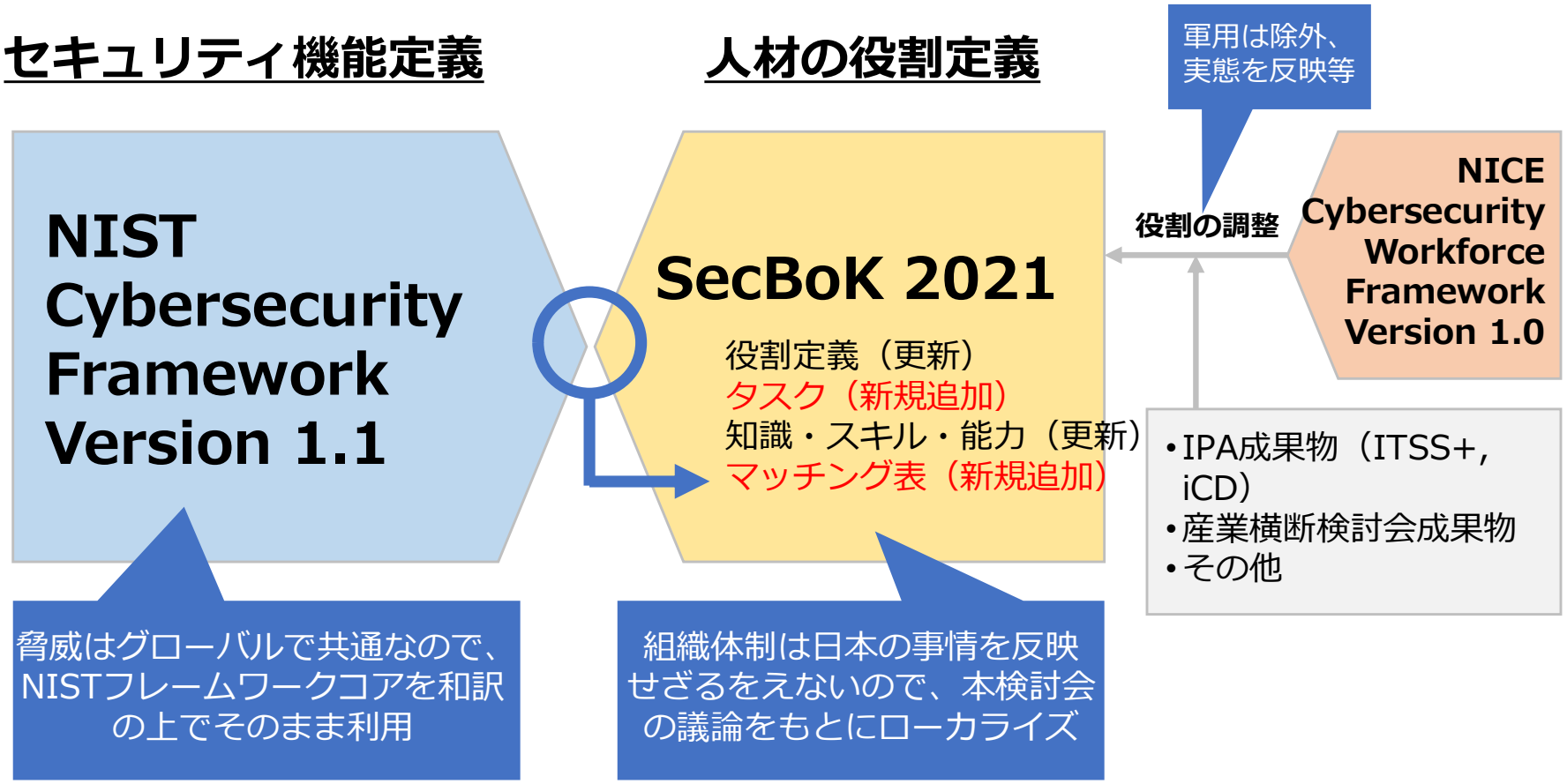
国際競争力を高めるためには、「人材」＋「デジタル」＋「セキュリティ」＝（つまり）**「セキュリティ人材の育成」**なき達成は不可能なことが明白です。

セキュリティ人材の育成は、国際競争力の向上に直結する施策である

セキュリティ知識分野

SecBoK（Security Body of Knowledge）とは

SecBoK2021改定の方法性
セキュリティ機能定義と役割定義の分析



SecBoK2019の特長（１）
NIST SP800-181との連携１

NIST SP800-181の約1000強のスキル項目とSecBoK2021の16ロールとの連携を実施（日本で使いやすいように、カテゴリー変更や、基礎・総論などの項目分けなどを独自に実施）

役割（ロール）

スキル項目

セキュリティ知識分野（SecBoK）人材スキルマップ2018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	ベンディング（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	新旧別	旧ID	分野	大項目	中項目	レベル	小項目	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	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
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					
18	K0060	旧NICEと同一	90	00基礎	3ソフトウェア		L	オペレーティングシステムに関する知識			2	1	1	1	1	1	1	1	1					1
19	K0068	旧NICEと同一	102	00基礎	3ソフトウェア		L	プログラミング言語の構造とロジックに関する知識						1	1	1	1		1					

SecBoK2021の特長（２）
NIST SP800-181との連携２

	役割（ロール）	役割定義（ユーザ企業におけるおもな役割）		NICE定義のロール名	NICEにおけるロールの定義
1	CISO （最高情報セキュリティ責任者）	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	許可権限者	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	幹部のサイバーリーダシップ	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投資/ポートフォリオ管理者	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。		（対応ロールなし）	
3	ノーティフィケーション	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。		（対応ロールなし）	
4	コマンダー	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	幹部のサイバーリーダシップ	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	トリアージ	事象に対する対応における優先順位を決定する。	27	幹部のサイバーリーダシップ	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	インシデントマネージャー	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	防衛インシデント対応者	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	インシデントハンドラー	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	防衛インシデント対応者	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	キュレーター	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	脅威/警告アナリスト	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	リサーチャー	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	サイバー防衛アナリスト	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	セルフアセスメント	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	システムセキュリティアナリスト	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	ソリューションアナリスト	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	システムセキュリティアナリスト	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	脆弱性診断士	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	脆弱性診断アナリスト	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	教育・啓発	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	サイバー教育カリキュラム開発者	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	サイバーセキュリティインストラクター	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	サイバーセキュリティ要員の育成者・管	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	フォレンジックエンジニア	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	法執行フォレンジックアナリスト	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	防衛フォレンジックアナリスト	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	インベスティゲーター	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	サイバー犯罪捜査員	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	リーガルアドバイザー	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	サイバーリーガルアドバイザー	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企画部門	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	サイバーセキュリティ対策方針・戦略の	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プロジェクトマネージャー	情報技術関連プロジェクトを直接管理する。
15	ITシステム部門	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	ネットワーク運用スペシャリスト	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	システムアドミニストレータ	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	情報システムセキュリティ管理者	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	通信セキュリティ管理者	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	サイバー防衛インフラサポートスペシャ	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	情報セキュリティ監査人	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プログラム監査者	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。

NIST　SP800-181の52ロールのうち、関連のあるロールをピックアップし、SecBoKの16ロールとの連携を実施

教育界（情報系大学）適用事例
コンピュータサイエンスカリキュラム標準（J17）

「プラス・セキュリティ人材」を育成するためには、情報系の学生全般にベーシックなセキュリティスキルを身に付けさせることも必要です。

情報専門学科カリキュラム標準（J07）とは、日本の情報専門教育の状況に対応した見直しを行い、コンピュータ科学（CS）情報システム（IS）コンピュータエンジニアリング（CE）ソフトウェアエンジニアリング（SE） インフォメーションテクノロジ（IT）一般情報処理教育（GE）についてまとめたカリキュラム標準で、2017年に見直しされJ17が公表されている。

人材に必要となるスキルについては、セキュリティ知識分野(SecBoK)人材スキルマップを参考とした。カリキュラムモデルに必要となる教えるべき知識項目の整理するため、サイバーセキュリティのカリキュラム作成の際に参考として、SecBoK人材スキルマップにおける各情報専門教育項目をカバーする範囲 の専門レベル を対象としたレベル分けを整理した。

分野｜大項目｜中項目	CS	IS	CE	SE	IT	GE	CyS ICT 基礎	CyS セキュリティ基礎	CyS セキュリティ専門
基礎｜ICT 基礎｜情報理論	●			●	●	●	●		
基礎｜ICT 基礎｜計算機ハードウェア	●	●		▲	●		●		
基礎｜ICT 基礎｜ネットワークインフラ	●	●		▲	●	●	●		
基礎｜ICT 基礎｜通信プロトコル・サービス	●	●		▲	●	●	●		
基礎｜ICT 基礎｜データ構造	●	●		▲	▲		●		
基礎｜ICT 基礎｜データベース	●	●		▲	●	●	●		
基礎｜ICT 基礎｜ナレッジマネジメント	●	●		▲	▲	●	●		
基礎｜ICT 基礎｜アルゴリズムとプログラミング	●			●	●	●	●		
基礎｜ICT 基礎｜オペレーティングシステム	●	●		▲	●	●	●		
基礎｜ICT 基礎｜ソフトウェア	●	●		●	●	●	●		
基礎｜ICT 基礎｜システム開発	●			●	●	●	●		
基礎｜ICT 基礎｜システム運用	▲	●		▲	●	●	●		

ASEAN諸国におけるSecBoK利活用 インドネシアおよびベトナムでの事例

独立行政法人国際協力機構（JICA）において、SecBoKを利用したセキュリティ人材育成プロジェクトが実施されている。

インドネシア：サイバーセキュリティ人材育成プロジェクト

https://www2.jica.go.jp/ja/evaluation/pdf/2018_1701288_1_s.pdf

【プロジェクト概要】
インドネシア最高峰の大学の一つであるインドネシア大学におい てプロフェッショナル（実務者）向けサイバーセキュリティ教育システムを立 上げることで、重要情報インフラ分野を中心とする民間機関や政府に対してサイバーセキュリ ティ人材を持続的に供給する。

【事業概要】
本事業は、インドネシア国において、**セキュリティ知識分野（SecBoK）人材スキルマップに準拠**するプロフェッショナル人材育成のためのサイバーセキュリティプログラムをインドネシア大学内に立上げ、諸外国のサイバーセキュリティ人材も巻込みながら、同大学におけるサイバーセキュリティ人材の育成システム強化を図り、民間機関・政府のサイバーセキュリティ対応能力強化に寄与するもの。

ベトナム：サイバーセキュリティに関する能力向上プロジェクト（キャリア開発計画）

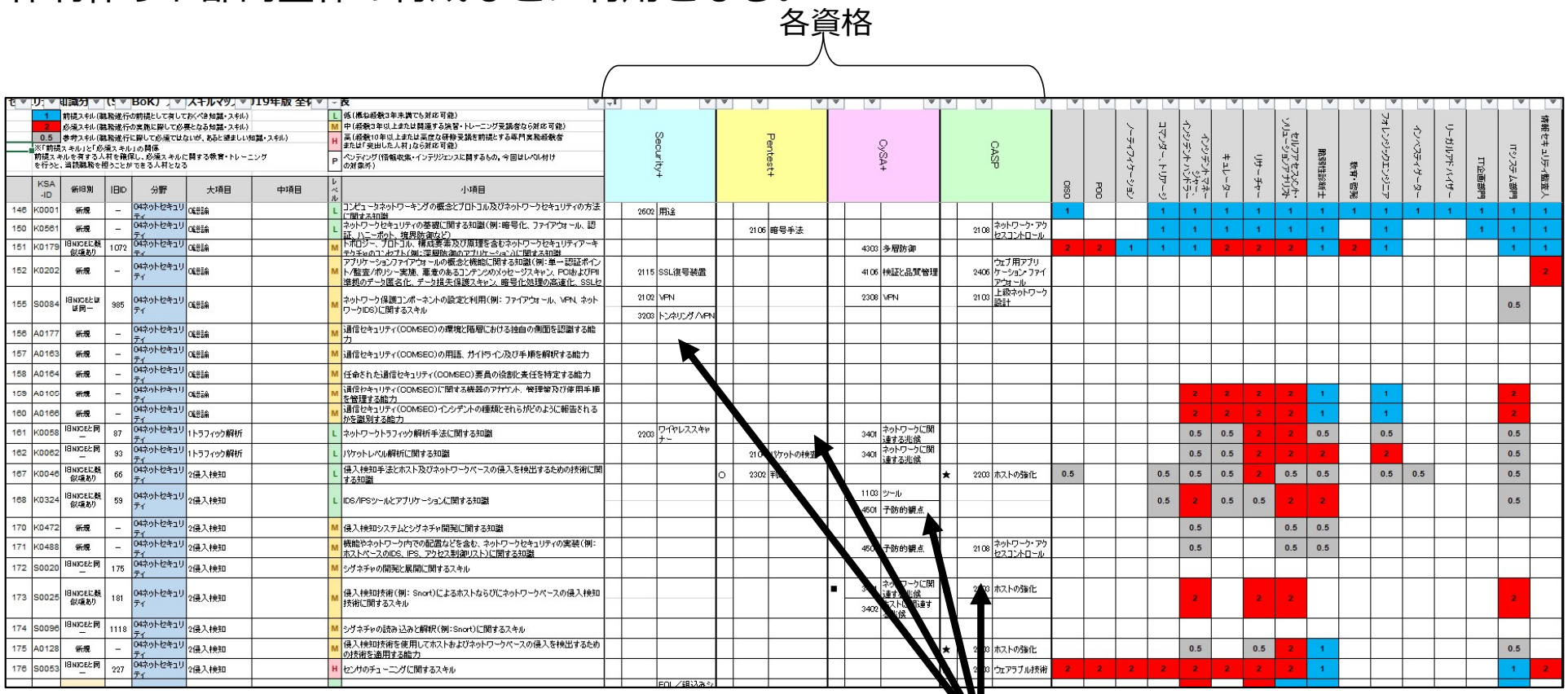
https://www2.jica.go.jp/ja/announce/pdf/20190424_190086_4_02.pdf

【プロジェクト概要】
ベトナム情報通信省より「サイバーセキュリティに関する能力向上プロジェクト」実施の要請がなされた。要請された内容は、政府サイバーセキ ュリティ人材の能力向上、政府情報ネットワークをサイバー攻撃から守る機材・技術 の供与、サイバーセキュリティ啓発活動などとなっている。

【活動概要】
SecBoK のフレームワークに定義された役割（ロール）のうち必要とされるものを明らかにし、それぞれの職員のキャリア開発計画を策定する。また**SecBoK のフレームワークに定義された役割（ロール）のうち優先度の高いもの研修コースを計画・実施**する

資格との連携事例
CompTIAセキュリティ関連資格とSecBoKスキル

ベンダーニュートラルなIT資格団体であるCompTIAにおいて、各資格で問われているスキル項目とSecBoKスキル項目とのマッピングを実施。これにより資格ホルダーがどのセキュリティロールに適合度が高いかなどか可視化され、個人の育成計画だけでなく部門や組織の体制作りや部門全体の育成などに有用となる。



SecBoK利用による プラス・セキュリティ人材育成

JNSA

プラス・セキュリティ人材育成に使いやすくなるよう、改訂

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

「プラス・セキュリティ人材」とは

ここから始まった
セキュリティ人材 20万人？不足

日本経済新聞

2016年6月4日（土）

Web刊 速報 ビジネスリーダー マーケット テクノロジー アジア スポーツ マネー・ライフ

全て 経済 企業 国際 政治 株・金融 スポーツ 社会 ニュース18時 その他ジャンル▼

速報＞経済＞記事

サイバー防衛で20万人不足　経産省調べ、20年に

2016/5/19 0:04 | 日本経済新聞 電子版

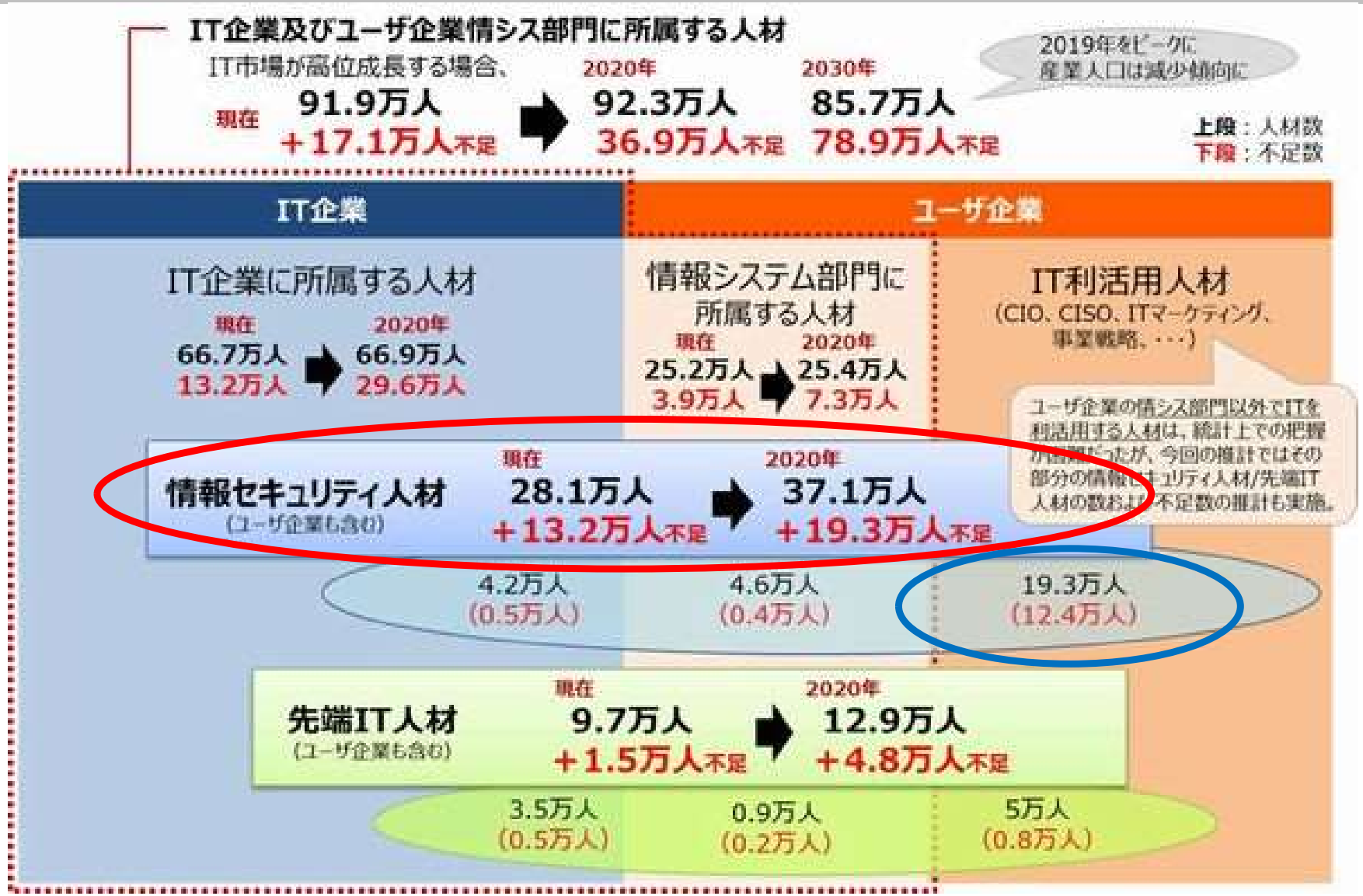
小 中 大　保存　リプリント　▼共有

経済産業省は、サイバー攻撃などに対処できるセキュリティーの専門人材が2020年に20万人近く不足するとの調査結果をまとめた。人工知能（AI）など最先端のIT（情報技術）に関わる人員も約5万人足りなくなる見通し。官民を挙げた人材育成が急務になる。

調査は企業へのアンケートやIT産業の就職・離職率、市場規模の統計などから、経産省が推計した。ITを主力とする企業だけでなく、自動車や電力など産業界全体で…

＜電子版トップ　＜速報トップ

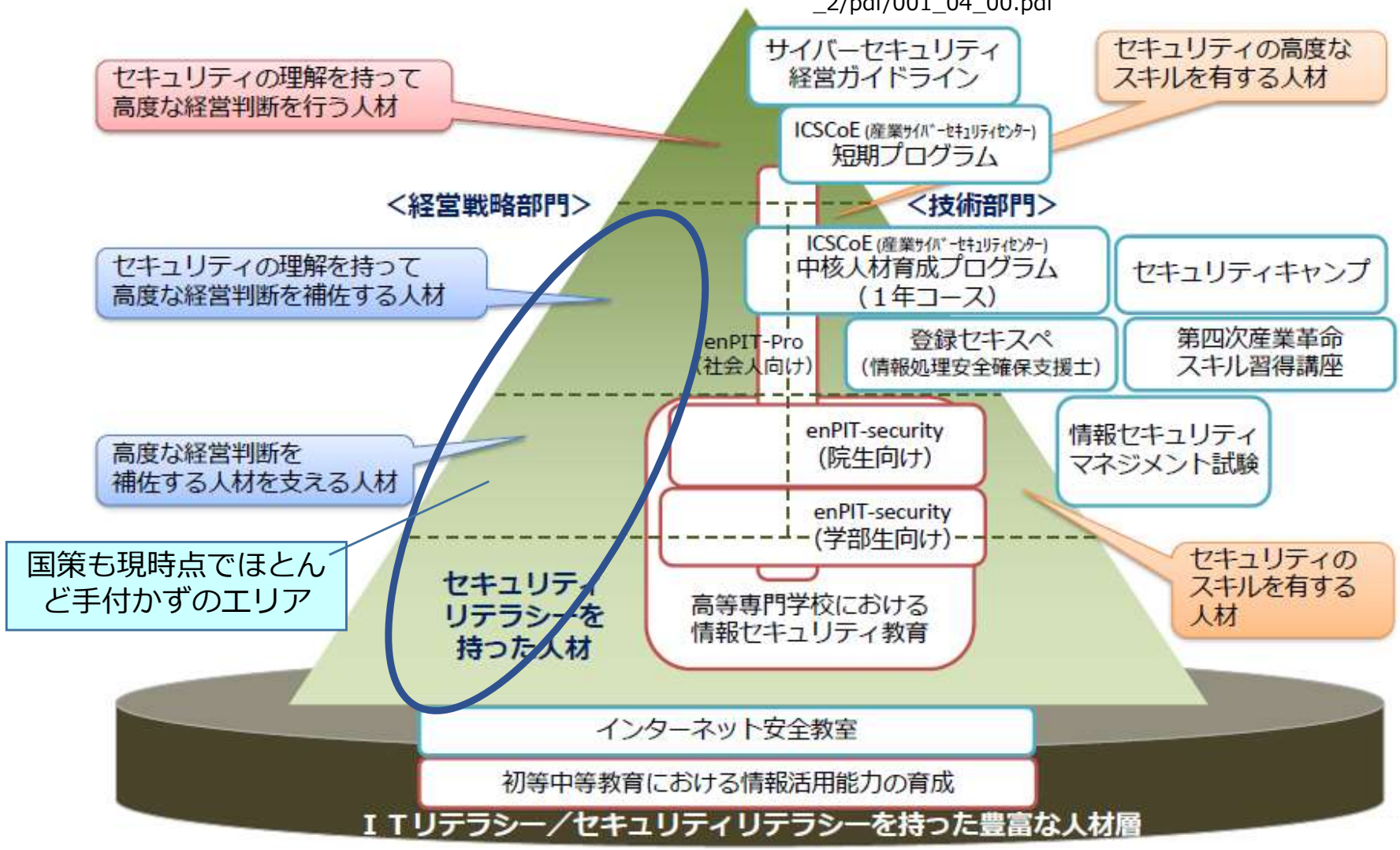
本当に足りない人材は？
ここの数値にも注目を



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

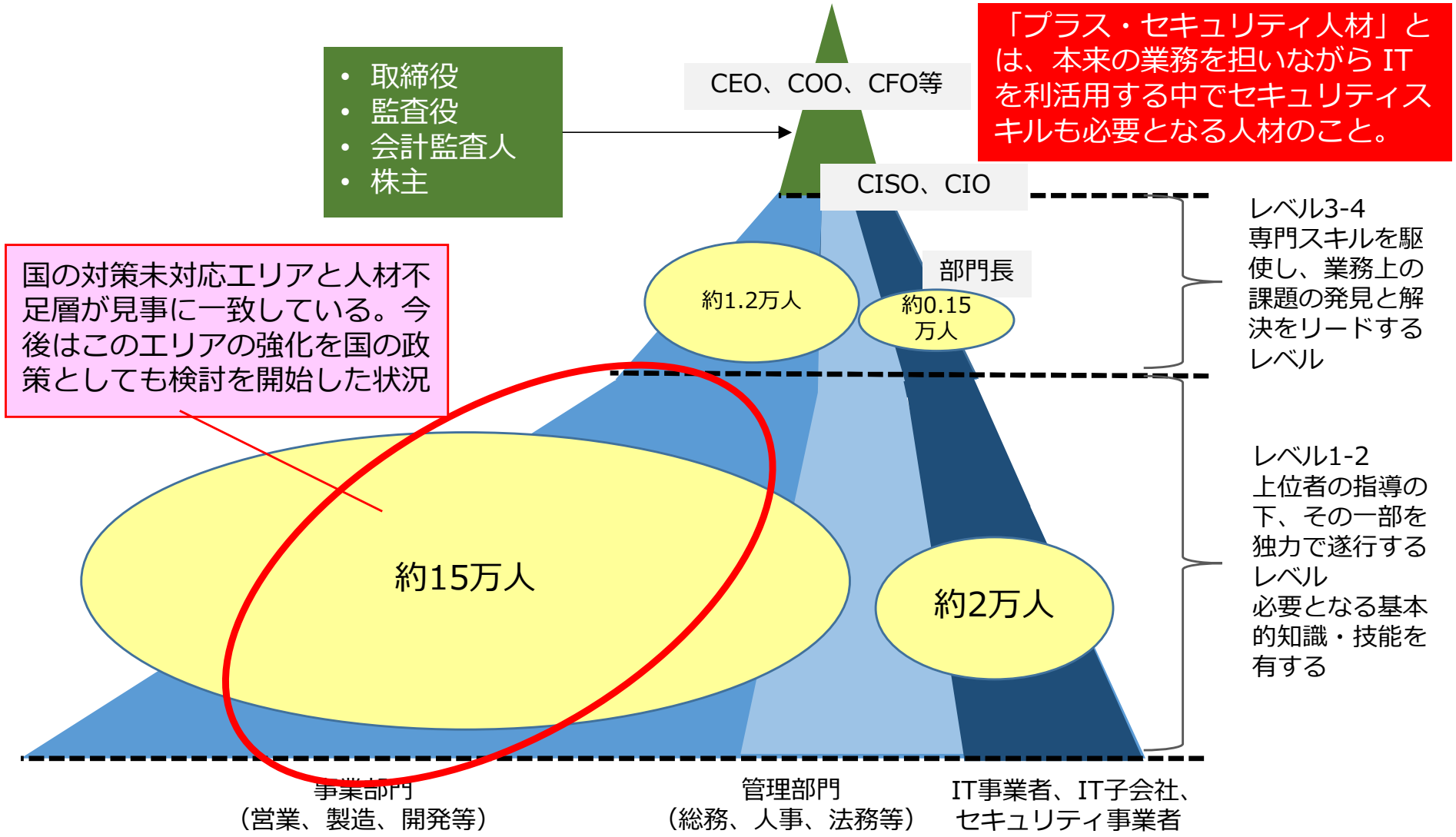
国では
どんな人材育成施策が取られていたのか

参照
http://www.meti.go.jp/committee/kenkyukai/shoujo/sangyo_cyber/wg_2/pdf/001_04_00.pdf

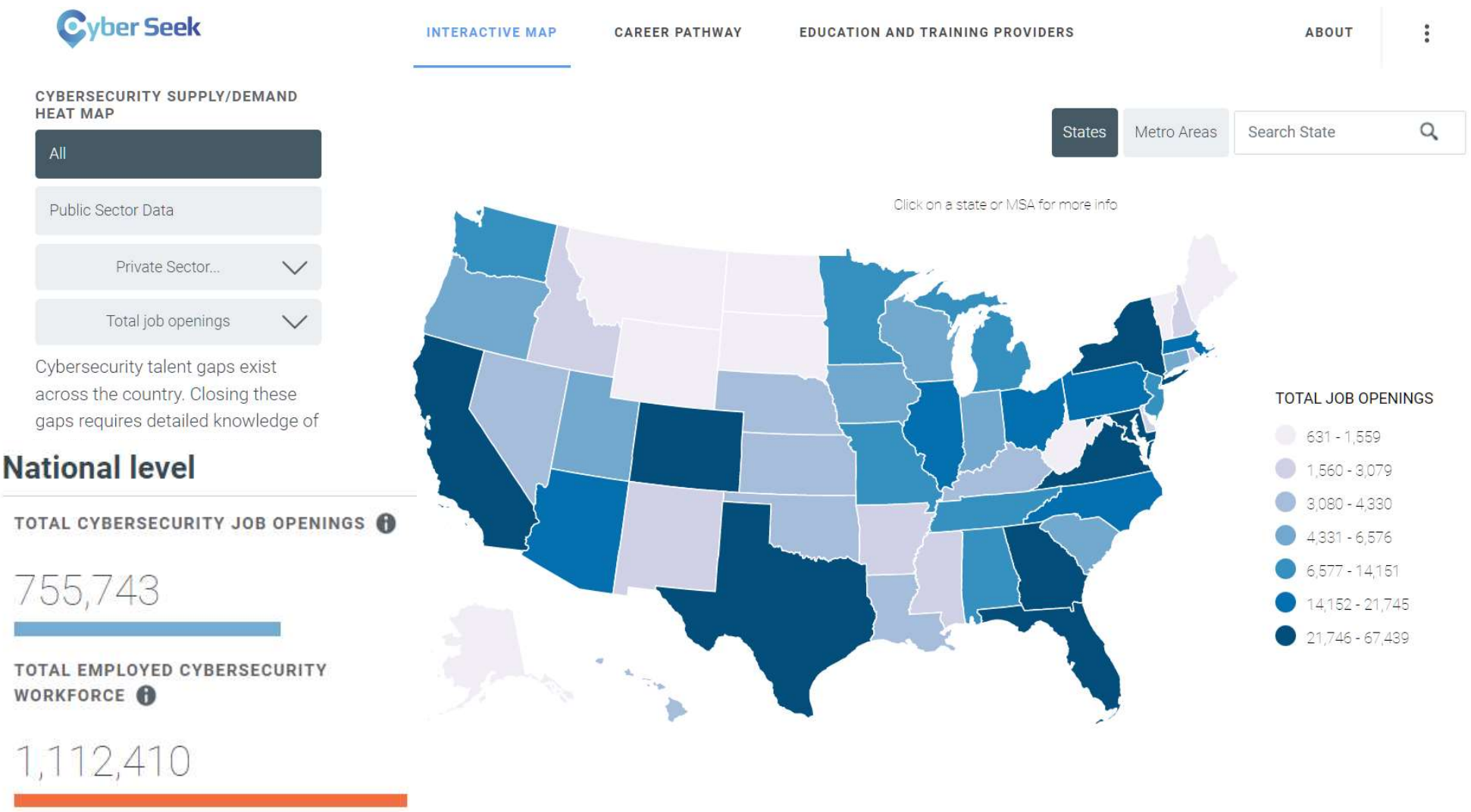


セキュリティ人材不足数を マッピングしてみると

「プラス・セキュリティ人材」不足への対応が必須である



日本だけではないセキュリティ人材不足



育成が必要な「プラス・セキュリティ人材とは」

「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/

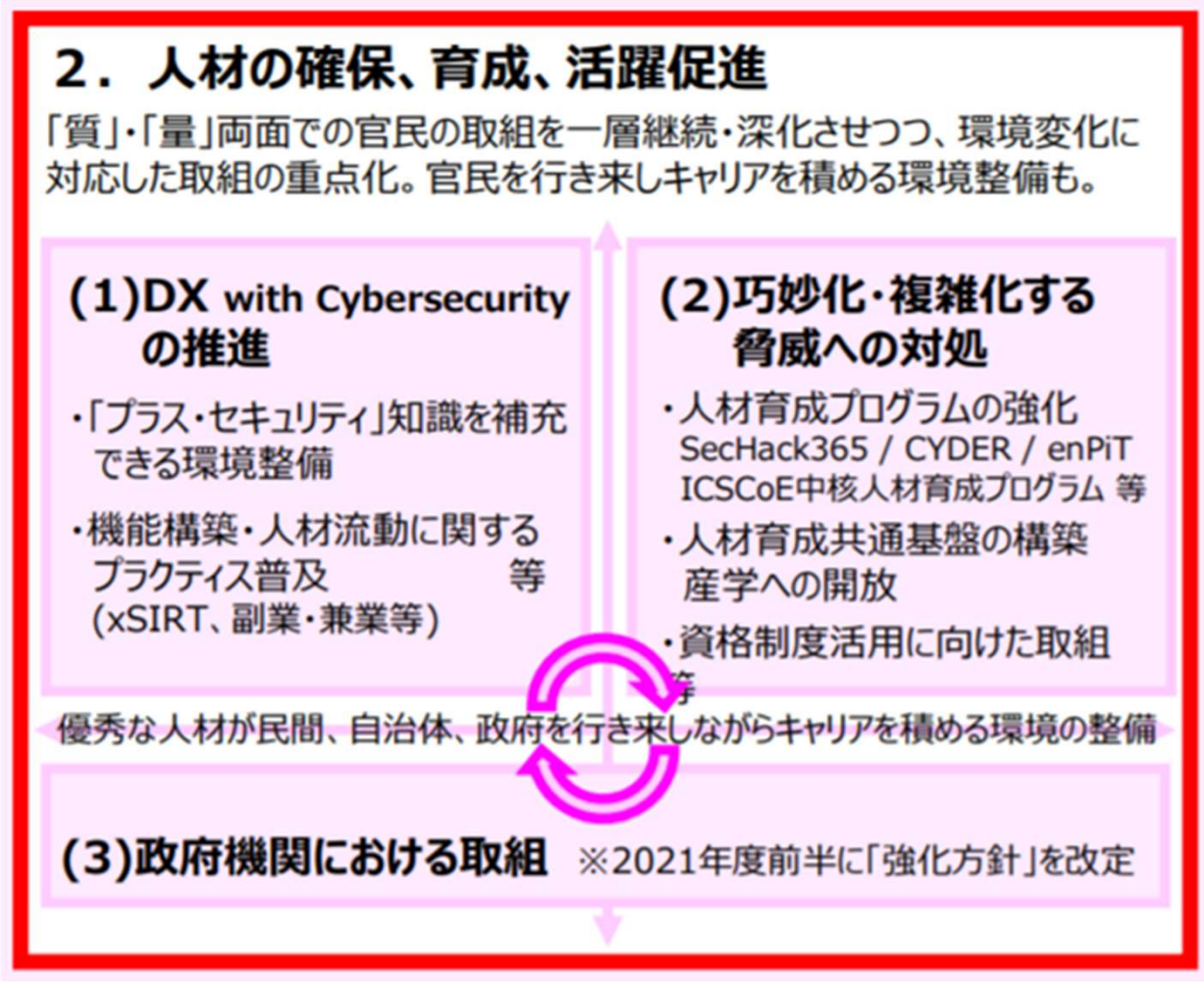
育成が必要な「プラス・セキュリティ人材とは」

「プラス・セ
活用する中で
不足しているの

IPA公開レポー
運用保守など)
このような人
バーセキュリ

IPAレポートを
リティにも携
の要になる「

サイバーセキュリティ戦略2021年
国においても、「プラス・セキュリティ」が



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）」

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

サイバー議連にも、「サプライチェーンセキュリティ」と「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。

経済産業省からは「体制構築・人材確保の手引き」概要

本書で扱う主要な概念の解説

セキュリティ統括機能

- 企業におけるリスクマネジメント活動の一部として、セキュリティ対策及びセキュリティインシデント対応について、CISOや経営層による意思決定や、事業部門におけるセキュリティ対策の検討及び実施について、専門的な知見や経験をもとにサポートする機能
- 経営層や各事業部門は、セキュリティ統括機能によるサポートを受けつつ、それぞれが責任を負うセキュリティ対策を実践する。
- 「機能」であって「組織」として設置しなくてもよい（企業組織の状況に応じて、最適な形態は異なる：以下は設置方法の例）
  - 独立した組織として設置
  - 管理部門の１機能として割当
  - 情シス部門の１機能として割当
  - 組織横断的な委員会形態で運用

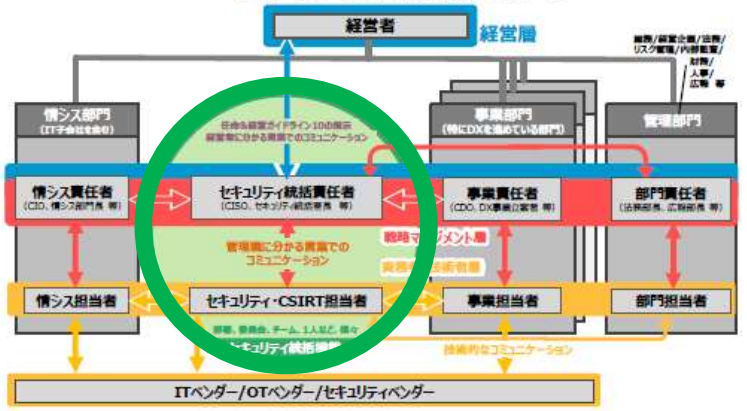
ITSS+（セキュリティ領域）

- 企業のセキュリティ対策に必要となる関連業務のまとまりを17分野に整理したもの
- セキュリティの専門性の高い分野だけでなく、経営層や法務部門、事業ドメインまで、サイバーセキュリティ対策に関わる幅広い領域を網羅している
- DXの取組を通じたクラウド化、アジャイル開発、開発・セキュリティ対策・運用の一体化（DevSecOps）等の動きの中、各分野の境界は曖昧化の傾向にある

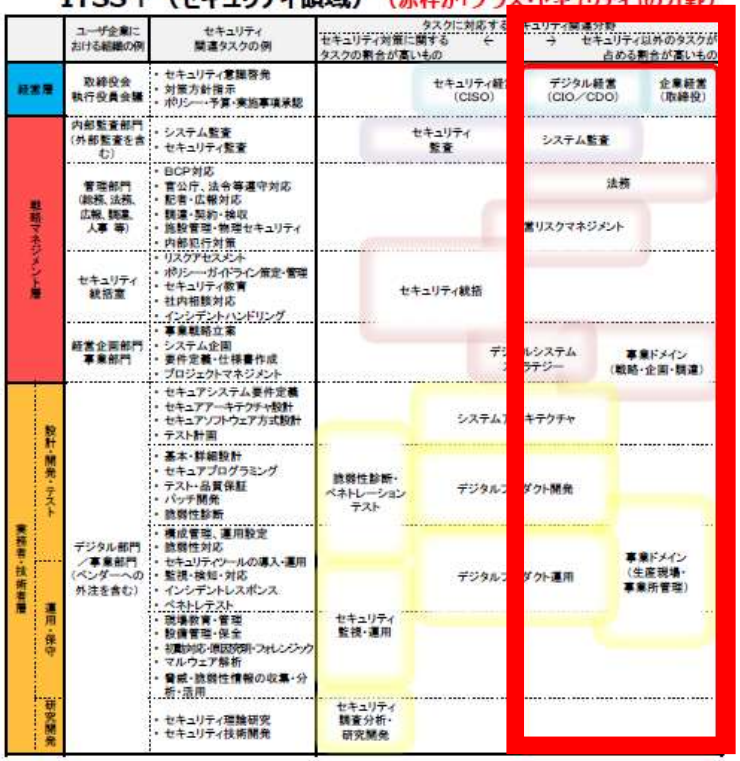
プラス・セキュリティ

- セキュリティ対策を本務としないが、業務遂行にあたってセキュリティを意識し、必要かつ十分なセキュリティ対策の実践が求められる業務が「プラス・セキュリティ」の対象
- 「プラス・セキュリティ」という人材が業務担当者と別に存在するわけではなく、これまでの業務担当者がサイバーセキュリティの知識・スキルを習得し、実践することを通じて対策を担う
- DXの取り組み有無に関わりなく、ITを活用するすべての企業において実践すべき

セキュリティ統括機能のイメージ



ITSS＋（セキュリティ領域）（赤枠が「プラス・セキュリティ」の分野）



「プラス・セキュリティ」と「DX」

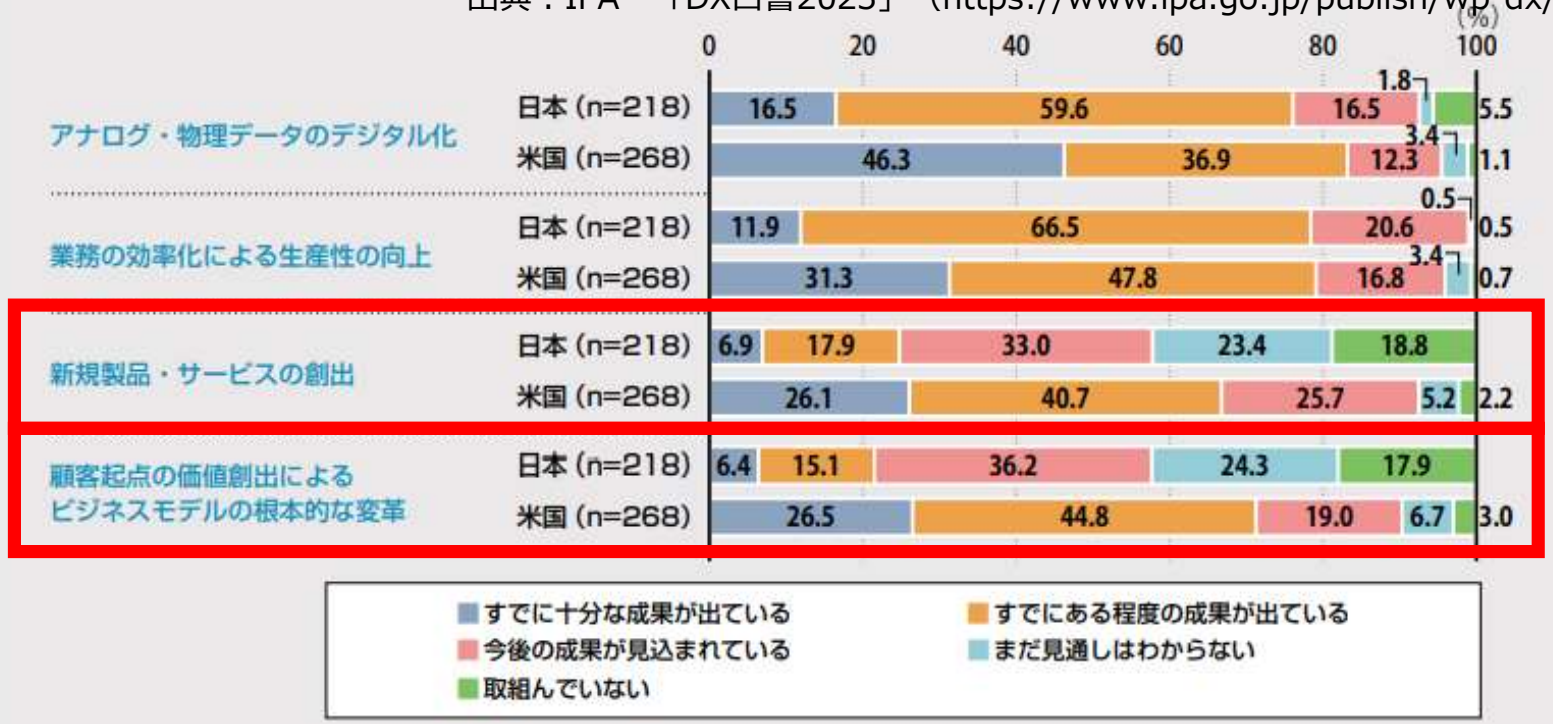
真のDX（デジタルトランスフォーメーション）とは、「ビジネスモデルや業務そのものの変革」を実現

DXとは、「製品やサービス、**ビジネスモデルを変革**するとともに、**業務そのもの**や、**組織、プロセス、企業文化・風土を変革**し、競争上の優位性を確立すること。」と定義されているが・・・

デジタルトランスフォーメーションに相当する「新規製品・サービスの創出」「顧客起点の価値創出によるビジネスモデルの根本的な変革」については20%台で、米国の約70%とは大きな差があり、デジタルトランスフォーメーションに向けてさらなる取組が必要である。

図表1-12 DXの取組内容と成果

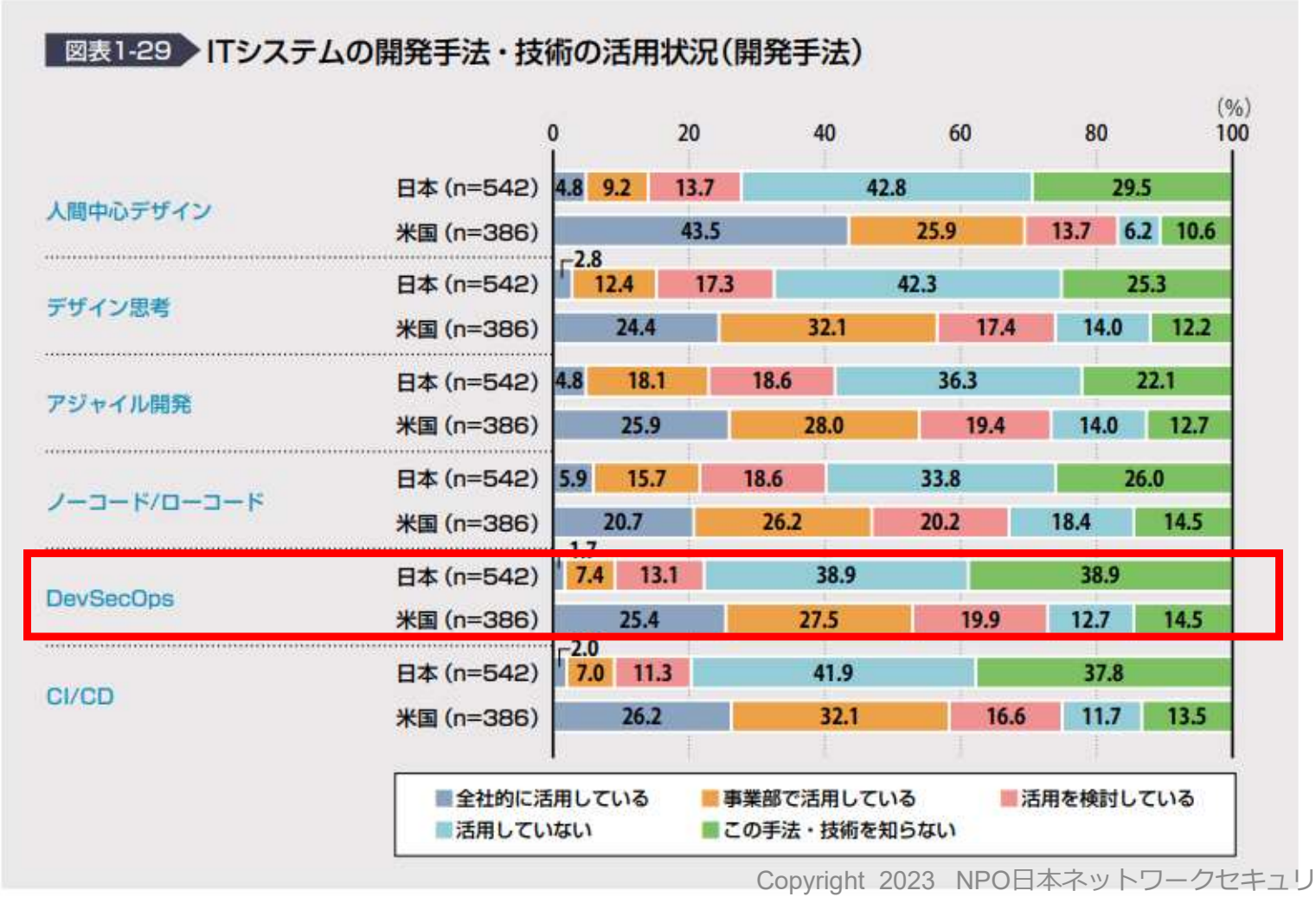
出典：IPA　「DX白書2023」（https://www.ipa.go.jp/publish/wp-dx/dx-2023.html）



DXを実現するための ITシステムの開発手法の活用状況

「全社的に活用している」「事業部で活用している」の合計）をみると、米国が4割半ばから7割弱に対して日本はおおむね1割から2割と、どの項目においても日米差が大きい。

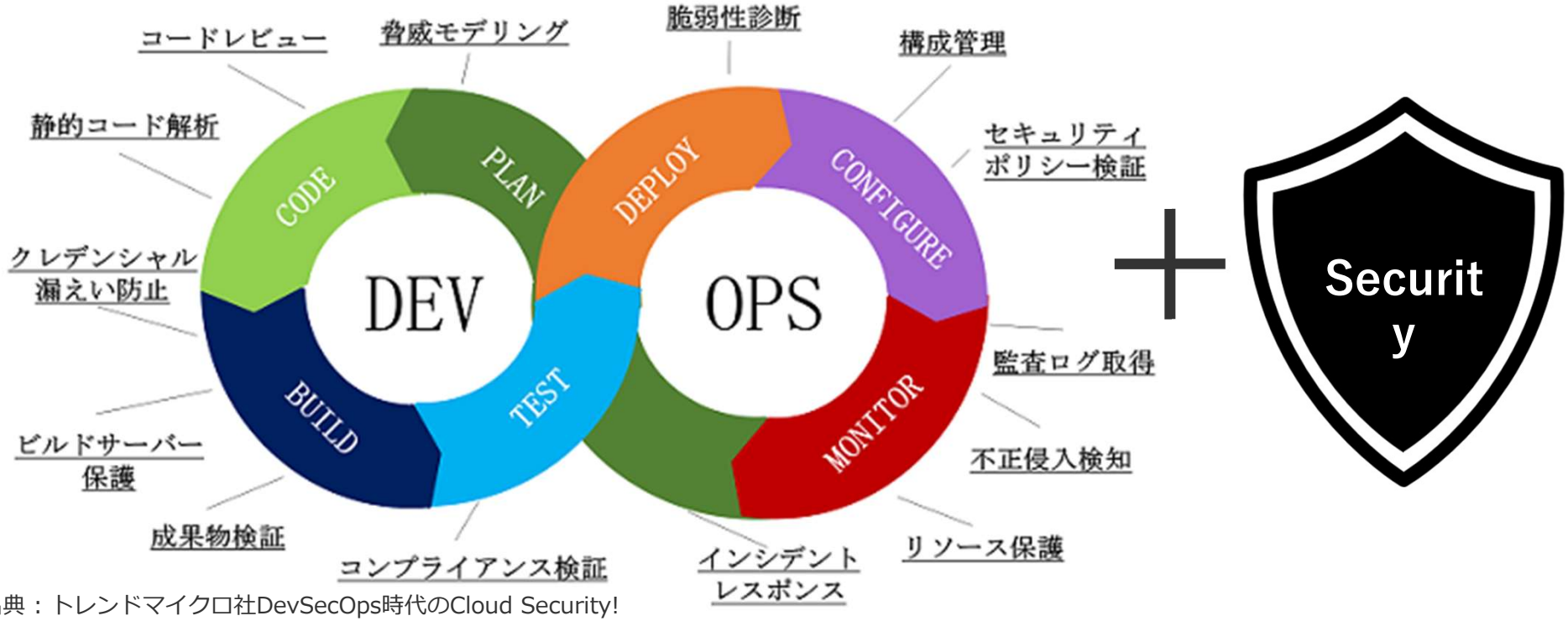
出典：IPA　「DX白書2023」（https://www.ipa.go.jp/publish/wp-dx/dx-2023.html）



DevSecOpsと攻めのプラス・セキュリティ人材

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**。

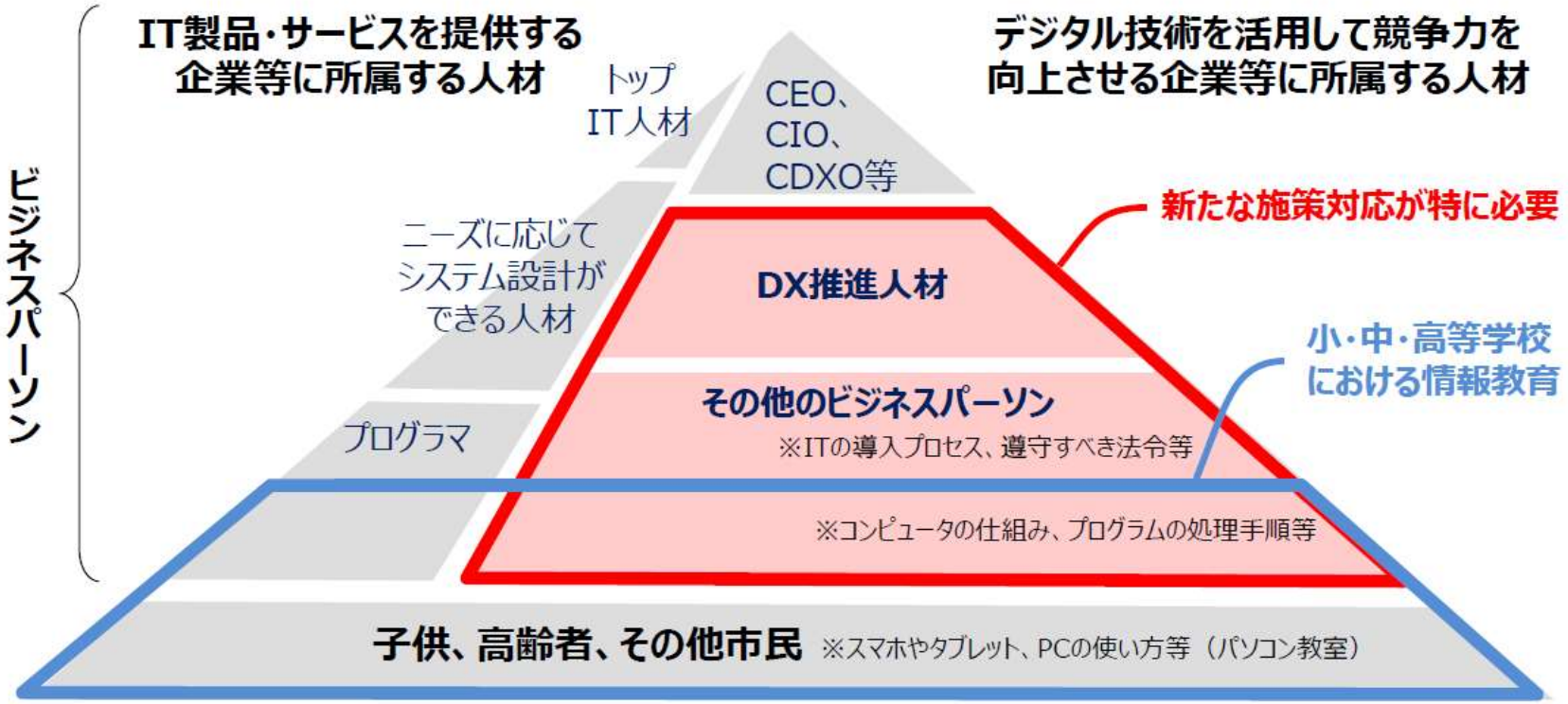


出典：トレンドマイクロ社DevSecOps時代のCloud Security!
https://www.trendmicro.com/ja_jp/business/campaigns/aws/resources/devsecops_whitepaper.html

国の考える、デジタル時代の人材像（まさにプラス・ICT人材）

デジタル社会における人材像

- デジタル社会においては、**全ての国民が、役割に応じた相応のデジタル知識・能力を習得**する必要がある。
- 若年層は、小・中・高等学校の情報教育を通じて一定レベルの知識を習得する。**現役のビジネスパーソンの学び直し（＝リスキリング）が重要**。

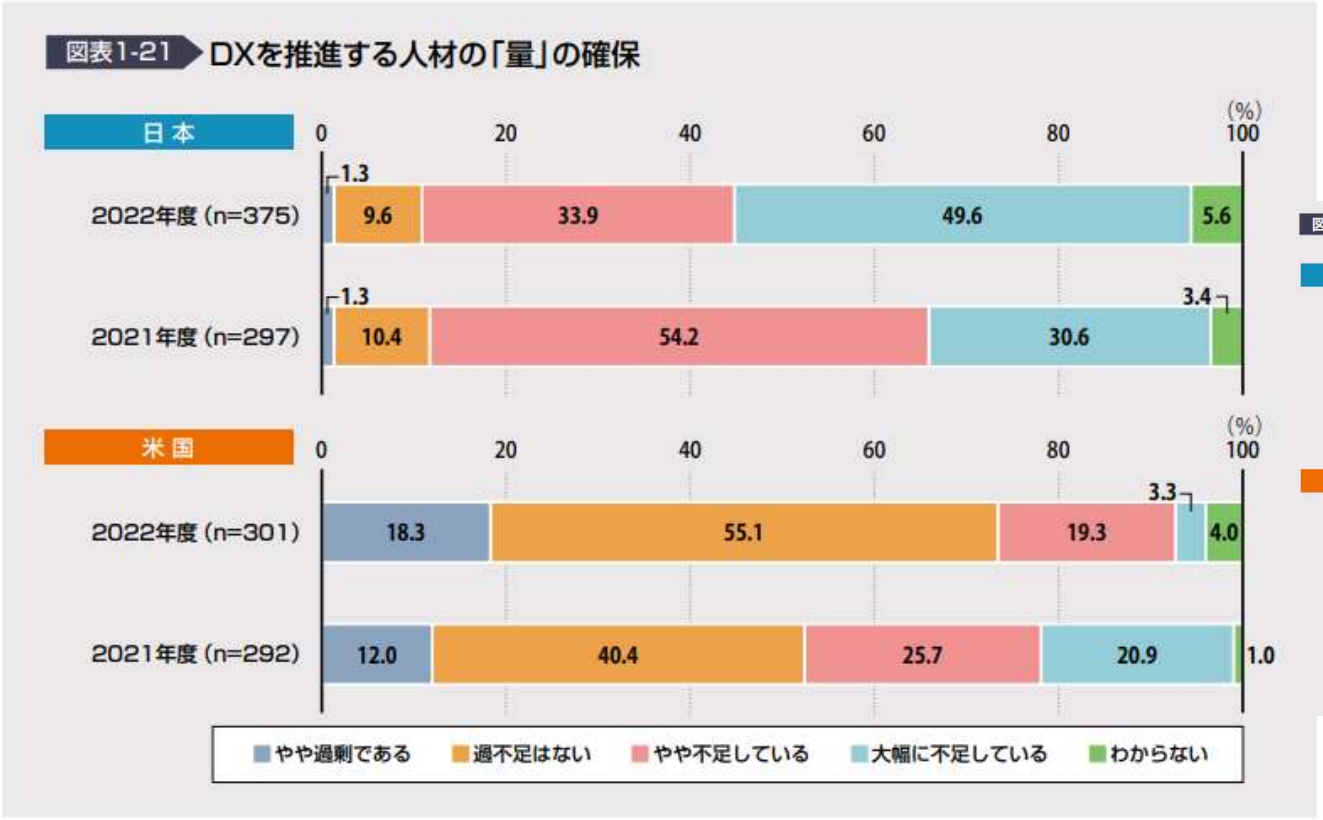


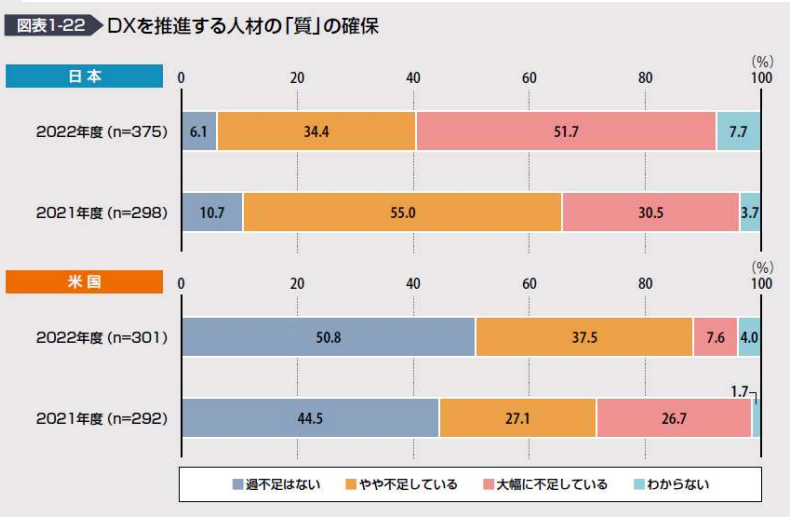
出典：経済産業省　デジタル時代の人材政策に関する検討会 実践的な学びの場 WG （第２回）資料

日本における大幅なDX人材不足

DXを推進する人材の「量」については、2022年度調査では、DXを推進する人材が充足していると回答した割合が日本は10.9%、米国は73.4%であった。「大幅に不足している」が米国では減少する一方、**日本では2021年度調査の30.6%から2022年度調査は49.6%と増加し、DXを推進する人材の「量」の不足が進んで**いる。
当然「質」も問題であるが、まずは「量」の対応が必要である。

出典：IPA　「DX白書2023」（https://www.ipa.go.jp/publish/wp-dx/dx-2023.html）





DXを進める企業等における ビジネスパーソンの人材像

JNSA

- DXのためには、まず**全てのビジネスパーソンがデジタルリテラシーを習得**することが重要。
- DXを推進する立場の人材は、**変革のためのマインドセットの理解・体得**した上で、**さらに専門的なデジタル知識・能力**が必要。

全てのビジネスパーソン

小・中・高等学校における**情報教育の内容**に加え、**ビジネスの現場でのデジタル技術の使い方の基礎**を学んだ人材

DX推進人材

DX推進のための組織変革に関する**マインドセットの理解・体得**が必要。

ビジネスアーキテクト	データサイエンティスト	エンジニア・オペレータ	サイバーセキュリティスペシャリスト	UI/UXデザイナー
デジタル技術を理解して、**ビジネスの現場においてデジタル技術の導入を行う全体設計**ができる人材	統計等の知識を元に、**AIを活用**して**ビッグデータから新たな知見を引き出し**、価値を創造する人材	クラウド等のデジタル技術を理解し、業務ニーズに合わせて必要な**ITシステムの実装やそれを支える基盤の安定稼働**を実現できる人材	業務プロセスを支える**ITシステムをサイバー攻撃の脅威から守る**セキュリティ専門人材	顧客との接点に**必要な機能とデザイン**を検討し、システムの**ユーザー向け設計**を担う人材

出典：経済産業省　デジタル時代の人材政策に関する検討会 実践的な学びの場 WG （第２回）資料

DXを支えるセキュリティ人材育成の課題

・DXを推し進めるのは、事業部門の参画が必須

・DXの実現は、「攻めのIT投資」となるので、セキュリティにも攻めの視点

・DXにおいては、DevSecOps開発が増えるため、事業部門にプラス・セキュリティ人材が必須

しかし・・・

・事業部門では、「プラス・セキュリティ」の評価ができない
・セキュリティ部門は、事業部門に手を出せない
・必要なセキュリティ人材の育成の仕方がわからない

経営視点より、全社施策として「プラス・セキュリティ人材」育成に取組み
人事部門を巻き込み、「プラス・セキュリティ」価値評価の実現が必要
育成すべき人材を明確にし、SecBoK利用での育成を！

まとめ：セキュリティ人材も新たなステージへ

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（ビジネス）視点から「攻めのセキュリティ」**登場。ユーザ・事業部門にもセキュリティ意識を

4．セキュリティ人材育成は、ITやセキュリティ部門だけの取り組みでない

プラス・セキュリティ人材は、事業部門にこそ多く必要なため、**経営部門や人事部門を巻き込んだ取り組みが必須**となる

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