

独立行政法人情報処理推進機構（IPA）
第2回 第4次産業革命に対応したスキル標準検討WG

ITSS+（プラス）案

平成29年2月23日

IPA 独立行政法人情報処理推進機構

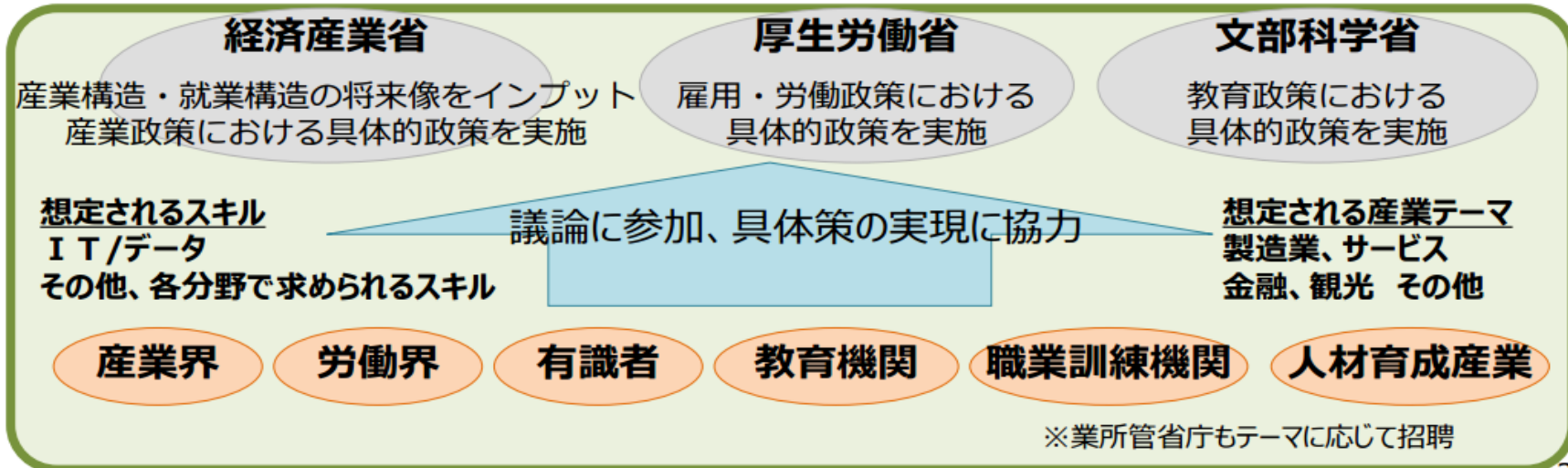
<全体> 第4次産業革命 人材育成推進会議 のスタート

- 関係省庁や産業界等の参加を得て、産業構造や社会構造の転換を踏まえ、各産業で求められるスキルや能力等の人材育成について検討し、各省庁が実施すべき具体的な施策に反映させるため、構造改革徹底推進会合の下に「第4次産業革命 人材育成推進会議」を開催。

<メンバー>

- | | | | |
|-------|-----------------------|----------------------------------|----------------------|
| ・金丸恭文 | フューチャー 代表取締役会長CEO【座長】 | ・永易 克典 | 三菱東京UFJ銀行相談役 |
| ・安宅和人 | ワージャパンCSO | ・大久保秀夫 | フォル代表取締役会長 |
| ・松尾豊 | 東京大学大学院工学系研究科准教授 | ・逢見直人 | 連合事務局長 |
| ・稲葉善治 | ファック(株)代表取締役会長兼CEO | ・石川正俊 | 東京大学情報理工学系研究科長 |
| ・岩本敏男 | NTTデータ代表取締役社長 | ・小杉礼子 | (独)労働政策研究・研修機構特任フェロー |
| ・牧野正幸 | ワークスアプリケーションズ代表取締役CEO | ・内閣官房再生事務局次長、経産省・厚労省・文科省・総務省担当局長 | |

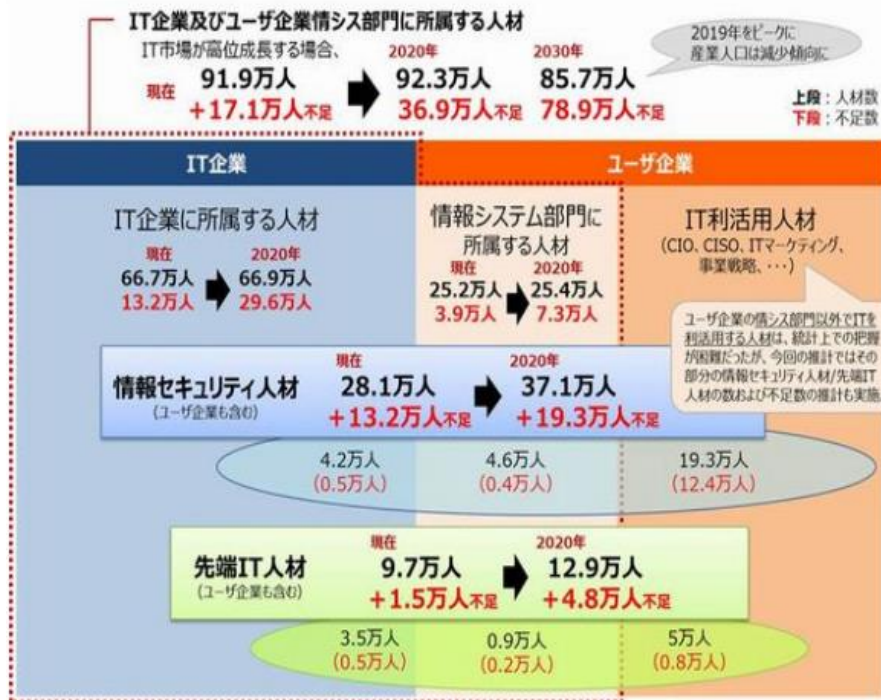
等



<全体> IT・データ人材需給 と ITスキル標準の全面改訂

- 分野別にブレイクダウンした「**人材需給調査**」と「**ITスキル標準の全面改訂**」を実施し、第4次産業革命に対応する「**能力・スキル**」や「**人材類型ごとの需給**」を明確化する。
- **緊急的に必要な措置、中長期的に必要な措置に分けて施策を講じていく。**

IT・データ人材の需給に関する推計の例



ITスキル標準の見直し

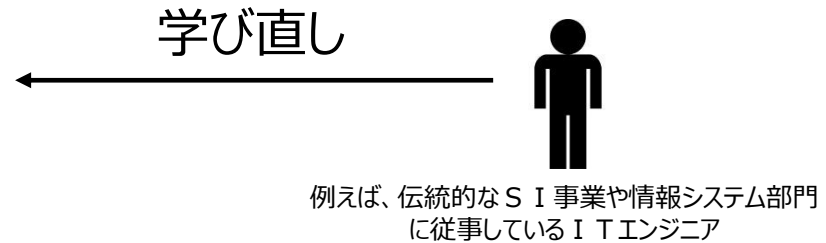
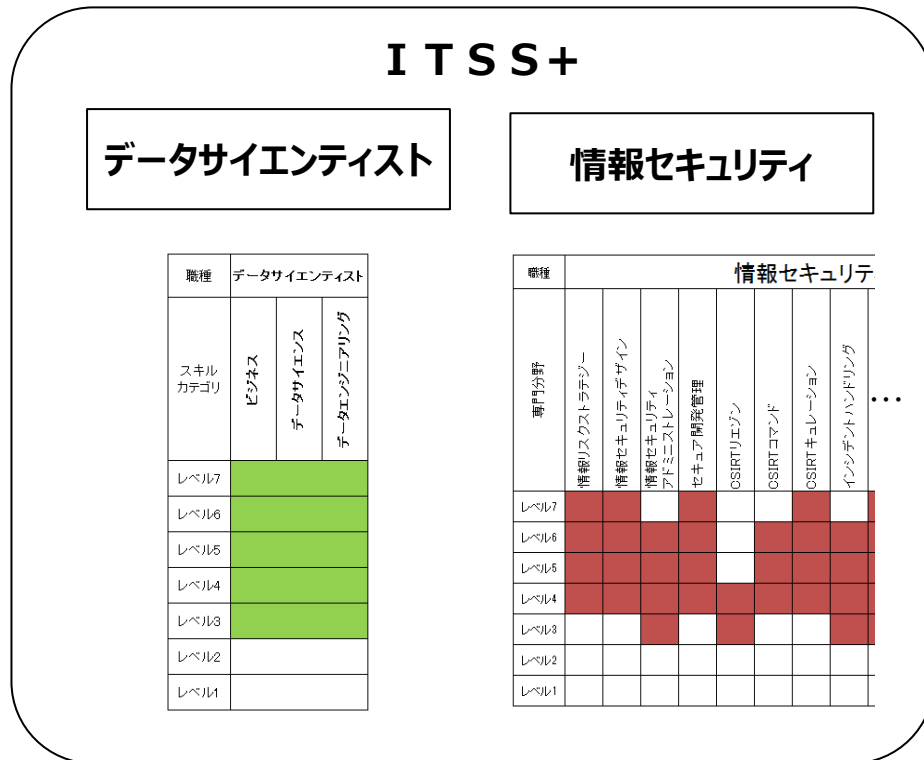
- 3月の中間とりまとめで、**データサイエンティスト、セキュリティに関連する人材タイプの拡充**を行う。
- 4月以降、新しいサービス・プロダクト開発手法等、第4次産業革命に伴い主流となる新技術に対応するIT人材に焦点をあてた検討を継続。

人材類型(11職種)×レベル(7段階)でIT人材を区分

職種	システム設計	ソフト開発	コンサルタント	...
レベル				
レベル7 世界で通用するブレイヤー				●今後、 データサイエンティスト に関連する人材タイプを拡充 (現在はない) ● セキュリティ に関する人材タイプも精緻化 (現在は各職種の中に含まれている)
...		ソフト開発のレベル4		
レベル1 最低限必要な基礎知識を保有				人材類型の見直しに合わせ、 ●人材が担う業務(タスク)及び持つべきスキル・知識を詳細に体系化した、iコンピテンシ・ディクショナリを拡充。(第4次産業革命に対応し、現在の約2800のタスク項目、約9900のスキル・知識項目を更に拡充)

ITSS+ (プラス) とは

- 既存のITエンジニアが、足元で必要性が高まっている分野に向けたスキル強化・転換を図るための学び直しに資することを目的に、既存のITSS、UISSに加えて活用されることを想定
- 足元で必要性が高まっている分野として「データサイエンティスト」「情報セキュリティ」を策定
- 3月末を目途に公表予定



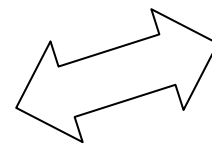
ITスキル標準 (ITSS)、ユーザスキル標準 (UISS)

職種	ITSS (Information Technology Skills Standard)										UISS (User Skills Standard)	
	ITSS-1	ITSS-2	ITSS-3	ITSS-4	ITSS-5	ITSS-6	ITSS-7	ITSS-8	ITSS-9	ITSS-10	UISS-1	UISS-2
レベル7												
レベル6												
レベル5												
レベル4												
レベル3												
レベル2												
レベル1												

ITSS+ (データサイエンティスト) の構成

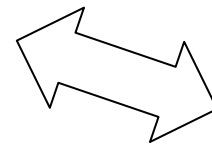
キャリア・フレームワーク

職種	データサイエンティスト		
	ビジネス	データサイエンス	データエンジニアリング
スキル カテゴリ			
レベル7		※	
レベル6		※	
レベル5			
レベル4			
レベル3			
レベル2			
レベル1			



必要なスキルの理解
スキル評価

スキルチェックリスト
(データサイエンティスト協会により公表)



活動の詳細な理解

タスク (データサイエンス)
(データサイエンティスト協会と連携し、新規作成中)

データサイエンティストのキャリア・フレームワーク案

- データサイエンティストが持つべきスキルのカテゴリ (“専門分野”ではない)
 - ✓ スキル評価におけるスキルチェックリストは、ビジネス、データサイエンス、データエンジニアリングの観点で整理している
 - ✓ 単独の一人がフルセットのスキルを持つのではなく、チームとして必要なスキルセットを実現する
 - ✓ 課題解決の対象によって核となるスキルは変わる
- 既存のITエンジニアの学び直しの観点から、レベル1、2は色を塗らない

職種/スキルカテゴリの説明

スキルチェックリスト(DS協会)のレベル

ITSS上のレベル定義

<職種>
データサイエンティスト
 データから価値を創出し、ビジネス課題に答えを出すプロフェッショナル

<スキルカテゴリ>
■ビジネス
 課題背景を理解した上で、ビジネス課題を整理し、解決する

■データサイエンス
 情報処理、人工知能、統計学などの情報科学系の知恵を理解し、活用する

■データエンジニアリング
 データサイエンスを意味のある形に使えるようにし、実装、運用する

業界を代表するレベル

棟梁レベル

独り立ちレベル

見習いレベル

職種	データサイエンティスト		
	ビジネス	データサイエンス	データエンジニアリング
スキルカテゴリ			
レベル7		※	
レベル6		※	
レベル5			
レベル4			
レベル3			
レベル2			
レベル1			

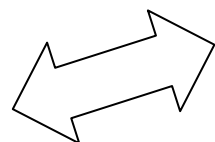
- ◆レベル7
 プロフェッショナルとしてスキルの専門分野が確立し、社内外において、テクノロジーやメソドロジ、ビジネスを創造し、リードするレベル。市場全体から見ても、**先進的なサービスの開拓や市場化をリード**した経験と実績を有しており、**世界で通用するプレーヤ**として認められる。
- ◆レベル6
 プロフェッショナルとしてスキルの専門分野が確立し、**社内外において**、テクノロジーやメソドロジ、ビジネスを創造し、リードするレベル。社内だけでなく市場においても、プロフェッショナルとして経験と実績を有しており、**国内のハイエンドプレーヤ**として認められる。
- ◆レベル5
 プロフェッショナルとしてスキルの専門分野が確立し、**社内において**、テクノロジーやメソドロジ、ビジネスを創造し、リードするレベル。
- ◆レベル4
プロフェッショナルとしてスキルの専門分野が確立し、自らのスキルを活用することによって、**独力で業務上の課題の発見と解決**をリードするレベル。
- ◆レベル3
要求された作業を全て独力で遂行する。スキルの専門分野確立を目指し、プロフェッショナルとなるために必要な応用的知識・技能を有する。
- ◆レベル2
 上位者の指導の下に、要求された作業を担当する。プロフェッショナルとなるために必要な基本的知識・技能を有する。
- ◆レベル1
 情報技術に携わる者に最低限必要な基礎知識を有する。

※ レベル6,7は、非構造データやドメイン等、特定の領域で突出し、これまでにない案を提示、実行する専門家となる。
 ITSS+では、学び直しの連続性の観点において、レベル5が現実的な上限になると想定

ITSS+ (情報セキュリティ) の構成

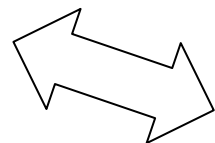
キャリア・フレームワーク

職種	情報セキュリティ														
	情報リスクストラテジ	情報セキュリティデザイン	セキュリティ開発管理	脆弱性診断	アドミニストレーション	情報セキュリティアナリシス	情報セキュリティ	OSIRTリエゾン	OSIRTコマンド	OSIRTキュレーション	インシデントハンドリング	情報セキュリティ監査	デジタルフォレンジクス	情報セキュリティインベステイション	情報セキュリティ
レベル7	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
レベル6	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
レベル5	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
レベル4	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
レベル3	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
レベル2	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
レベル1	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■



必要なスキルの理解

スキル
(iCD準拠、項目の一部追加 (作成中))



活動の詳細な理解

タスク
(iCD準拠、項目の一部追加 (作成中))

情報セキュリティのキャリア・フレームワーク案

- ユーザ企業、セキュリティベンダに関わらず※、情報セキュリティに関する専門スキルを持つ人材が担う業務分野の観点から整理（※CSIRTリエゾン、CSIRTコマンドはユーザ企業のみ）
- 既存のITエンジニアの学び直しの観点、及び情報処理安全確保支援士との関係（後述）から、レベル1、2は色を塗らない

職種	情報セキュリティ													
	情報リスクストラテジ	情報セキュリティデザイン	セキュア開発管理	脆弱性診断	アドミニストレーション	情報セキュリティ	アナリティクス	CSIRTリエゾン	CSIRTコマンド	CSIRTキュレーション	インシデントハンドリング	情報セキュリティ監査	デジタルフォレンジクス	情報セキュリティインベステイゲーション
レベル7														
レベル6														
レベル5														
レベル4														
レベル3														
レベル2														
レベル1														

情報セキュリティの専門分野の説明案

専門分野	説明
情報リスクストラテジ	自組織または受託先における業務遂行の妨げとなる情報リスクを認識し、その影響を抑制するための、組織体制の整備や各種ルール整備等を含む情報セキュリティ戦略やポリシーの策定等を推進する。自組織または受託先内の情報セキュリティ対策関連業務全体を俯瞰し、アウトソース等を含むリソース配分の判断・決定を行う。
情報セキュリティデザイン	「セキュリティバイデザイン」の観点から情報システムのセキュリティを担保するためのアーキテクチャやポリシーの設計を行うとともに、これを実現するために必要な組織、ルール、プロセス等の整備・構築を支援する。
セキュア開発管理	情報システムや製品に関するリスク対応の観点に基づき、機能安全を含む情報セキュリティの側面から、企画・開発・製造・保守などにわたる情報セキュリティライフサイクルを統括し、対策の実施に関する責任をもつ。
脆弱性診断	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。
情報セキュリティアドミニストレーション	組織としての情報セキュリティ戦略やポリシーを具体的な計画や手順に落とし込むとともに、対策の立案や実施（指示・統括）、その見直し等を通じて、自組織または受託先における情報セキュリティ対策の具体化や実施を統括する。また、利用者に対する情報セキュリティ啓発や教育の計画を立案・推進する。
情報セキュリティアナリシス	情報セキュリティ対策の現状に関するアセスメントを実施し、あるべき姿とのギャップ分析をもとにリスクを評価した上で、自組織または受託先の事業計画に合わせて導入すべきソリューションを検討する。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。
CSIRTリエゾン	自組織外の関係機関、自組織内の法務、渉外、IT部門、広報、各事業部等との連絡窓口となり、情報セキュリティインシデントに係る情報連携及び情報発信を行う。必要に応じてIT部門とCSIRTの間での調整の役割を担う。
CSIRTコマンド	自組織で起きている情報セキュリティインシデントの全体統制を行うとともに、事象に対する対応における優先順位を決定する。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。
CSIRTキュレーション	情報セキュリティインシデントへの対策検討を目的として、セキュリティイベント、脅威や脆弱性情報、攻撃者のプロファイル、国際情勢、メディア動向等に関する情報を収集し、自組織または受託先に適用すべきかの選定を行う。
インシデントハンドリング	自組織または受託先におけるセキュリティインシデント発生直後の初動対応（被害拡大防止策の実施）や被害からの復旧に関する処理を行う。セキュリティベンダーに処理を委託している場合は指示を出して連携する。情報セキュリティインシデントへの対応状況を管理し、CSIRTコマンドのタスクを担当する者へ報告する。
情報セキュリティ監査	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。
デジタルフォレンジクス	悪意をもつ者による情報システムやネットワークをを対象とした活動の証拠保全を行うとともに、消されたデータを復元したり、痕跡を追跡したりするための体系的な鑑識、精密検査、解析、報告を行う。
情報セキュリティインベスティゲーション	情報セキュリティインシデントを対象として、外部からの犯罪、内部犯罪を捜査する。犯罪行為に関する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の絞り込みを行う。

情報処理安全確保支援士との関係

- I T S S +における「情報セキュリティ」の対象範囲は、情報処理安全確保支援士の活動領域を包含する
- そのため、I T S S +で定義する職種の人材（及び目指す人材）にとって、情報処理安全確保支援士の取得は一定の能力証明として有用
- また、既に情報処理安全確保支援士の資格を持つ者にとっては、実務上、I T S S +によって具体的な自分の専門性を説明することが可能となる

職種	情報セキュリティ													
	情報リスクストラテジ	情報セキュリティデザイン	セキュリティ開発管理	脆弱性診断	アドミニストレーション	情報セキュリティ	アナリティクス	OSIRTリエゾン	OSIRTコマンド	OSIRTキュレーション	インシデントハンドリング	情報セキュリティ監査	デジタルフォレンジクス	情報セキュリティイシュー
レベル7														
レベル6														
レベル5														
レベル4														
レベル3														
レベル2														
レベル1														

= 情報処理安全確保支援士の想定業務

サイバーセキュリティに関する専門的な知識・技能を活用して企業や組織における安全な情報システムの企画・設計・開発・運用を支援し、サイバーセキュリティ対策の調査・分析・評価やその結果に基づく指導・助言を行う