経済産業省

第４次産業革命に向けたＩＴ人材育成とセキュリティ人材確保の重要性

(経済産業省ＩＴ人材育成施策)

平成３０年２月２７日

経済産業省商務情報政策局

情報技術利用促進課

地域情報化人材育成推進室

Connected Industries とは？

様々な業種、企業、人、機械、データなどがつながって

AI等によって、新たな付加価値や製品・サービスを創出、生産性を向上

高齢化、人手不足、環境・エネルギー制約などの社会課題を解決

これらを通じて、産業競争力の強化

→国民生活の向上・国民経済の健全な発展

こうしたコネクティッド・インダストリーズの実現は、業種・業態やこれまでのIT化の取組み度合いなどによって、多種多様。
一工場内の「つながり」にとどまるものもあれば、取引先や同業他社とつながったり、顧客や市場と直接つながっていくものも。
既存の関係を越えてつながりが広がれば、新たな産業構造の構築に至る可能性も。

Connected Industriesの考え方

～我が国産業が目指す姿（コンセプト）～

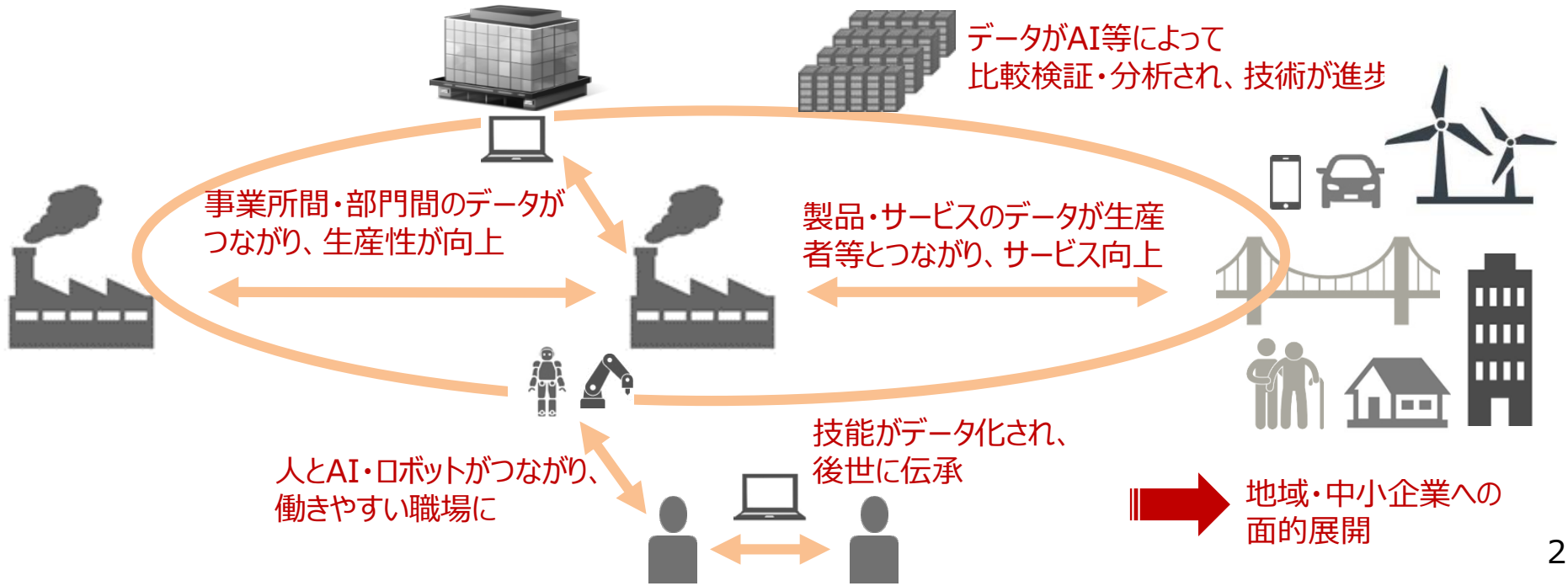
従来 事業所・工場、技術・技能等の電子データ化は進んでいるが、それぞれバラバラに管理され、連携していない

産学官における議論喚起・検討

- モビリティ、ものづくり、バイオ・素材、プラント保安、スマートライフなど分野別の取組
- データ利活用、標準化、IT人材、サイバーセキュリティ、AI開発など横断的な取組

将来 データがつながり、有効活用されることにより、技術革新、生産性向上、技能伝承などを通じた課題解決へ

「Connected Industries」は、Made in Japan、産業用ロボット、カイゼン等に続く、日本の新たな強みに



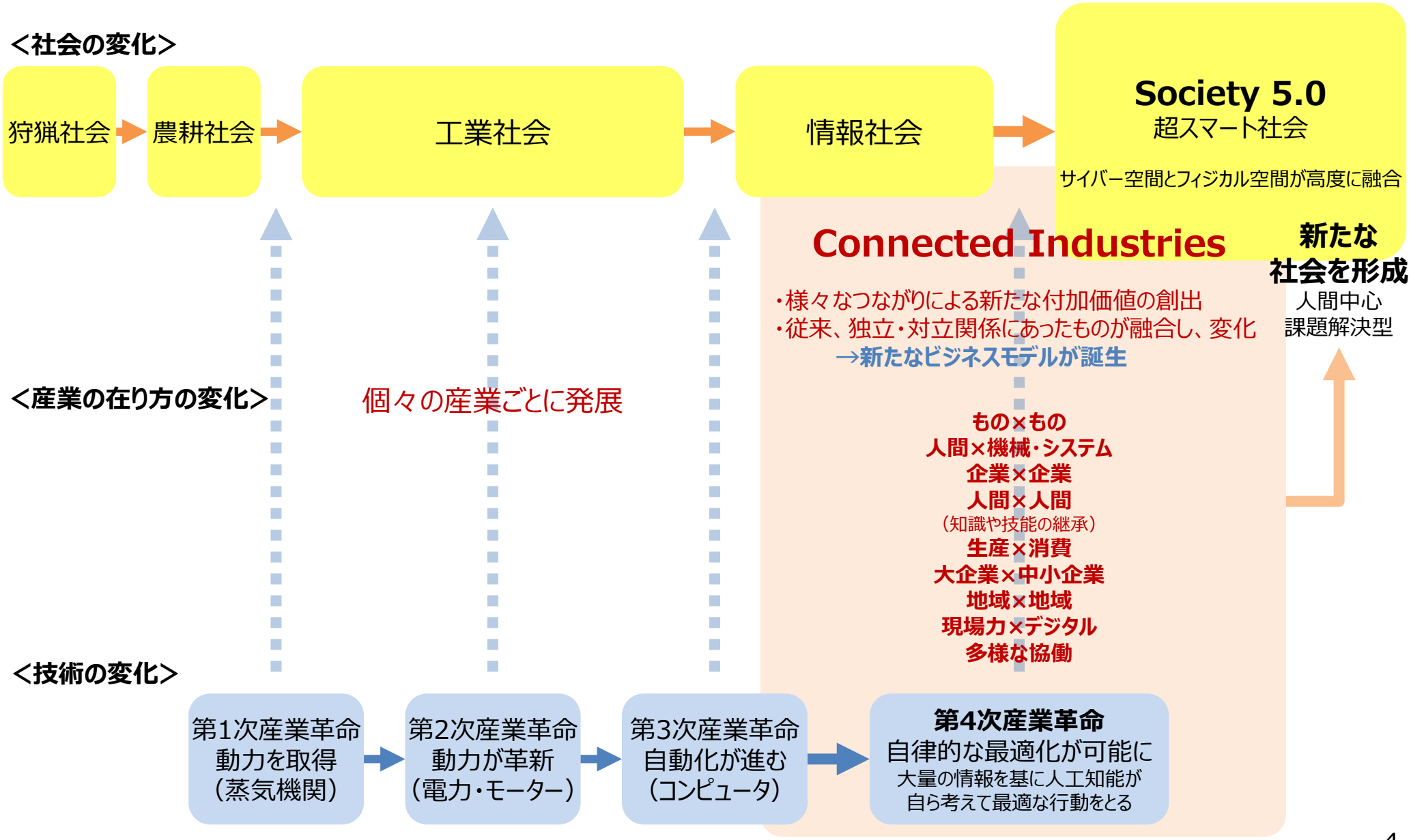
【参考】 CeBITにおける「Connected Industries」の発信

- 2017年3月に開催されたドイツ情報通信見本市（CeBIT）に、我が国はパートナー国として参加。**安倍総理、世耕経済産業大臣**他が出席。日本企業も**118社出展**（過去最大規模）。
- 安倍総理からは、我が国が目指す産業の在り方としての**「Connected Industries」のコンセプト**について、**①人と機械・システムが協調する新しいデジタル社会の実現**、**②協力や協働を通じた課題解決**、**③デジタル技術の進展に即した人材育成の積極推進**を柱とする旨をスピーチ。
- また、第四次産業革命に関する**日独共同声明「ハノーバー宣言」**が、世耕経済産業大臣、高市総務大臣、ツィプリス独経済エネルギー大臣との間で署名・発表。この中で、**人、機械、技術が国境を越えてつながる「Connected Industries」**を進めていく旨を宣言。

安倍総理のスピーチ

世耕経済産業大臣とツィプリス経済エネルギー大臣との会談

Society 5.0につながるConnected Industries



「Connected Industries」５つの重点取組分野

「自動走行・モビリティサービス」

- データ協調の在り方を早急に整理
- AI開発・人材育成の強化
- 物流等も含むモビリティサービスやEV化の将来像を見据えた取組

「ものづくり・ロボティクス」

- データ形式等の国際標準化
- サイバーセキュリティ・人材育成等の協調領域での企業間連携の強化
- 中小企業向けのIoTツール等の基盤整備

「バイオ・素材」

- 協調領域におけるデータ連携の実現
- 実用化に向けたAI技術プラットフォームの構築
- 社会的受容性の確保

「プラント・インフラ保安」

- IoTを活用した自主保安技術の向上
- 企業間のデータ協調に向けたガイドライン等の整備
- さらなる規制制度改革の推進

「スマートライフ」

- ニーズの掘り起こし、サービスの具体化
- 企業間アライアンスによるデータ連携
- データの利活用に係るルール整備

これらを支える横断的支援策を早急に整備

「Connected Industries」の横断的な政策

リアルデータの共有・利活用

- データ共有事業者の認定制度の創設、税制等による支援
- リアルデータをもつ大手・中堅企業とAIベンチャーとの連携によるAIシステム開発支援
- 実証事業を通じたモデル創出・ルール整備
- 「データ契約ガイドライン」の改訂

データ活用に向けた基盤整備
＜研究開発、人材育成、ｻｲﾊﾞｰｾｷｭﾘﾃｨ＞

- 革新的なAIチップ開発の促進
- ネット×リアルのハイブリッド人材、AI人材等の育成強化
- 世界中から優秀な人材を集める枠組みの検討
- サイバーセキュリティ対策の強化

さらなる展開
＜国際、ベンチャー、地域・中小企業＞

- 欧州、アジア等世界各国との協力強化
- 国際連携WGを通じたシステム輸出強化
- 国際標準化人材の質的・量的拡充
- 日本版ベンチャーエコシステムの実現
- 専門家育成や派遣による、地域・中小企業への支援強化

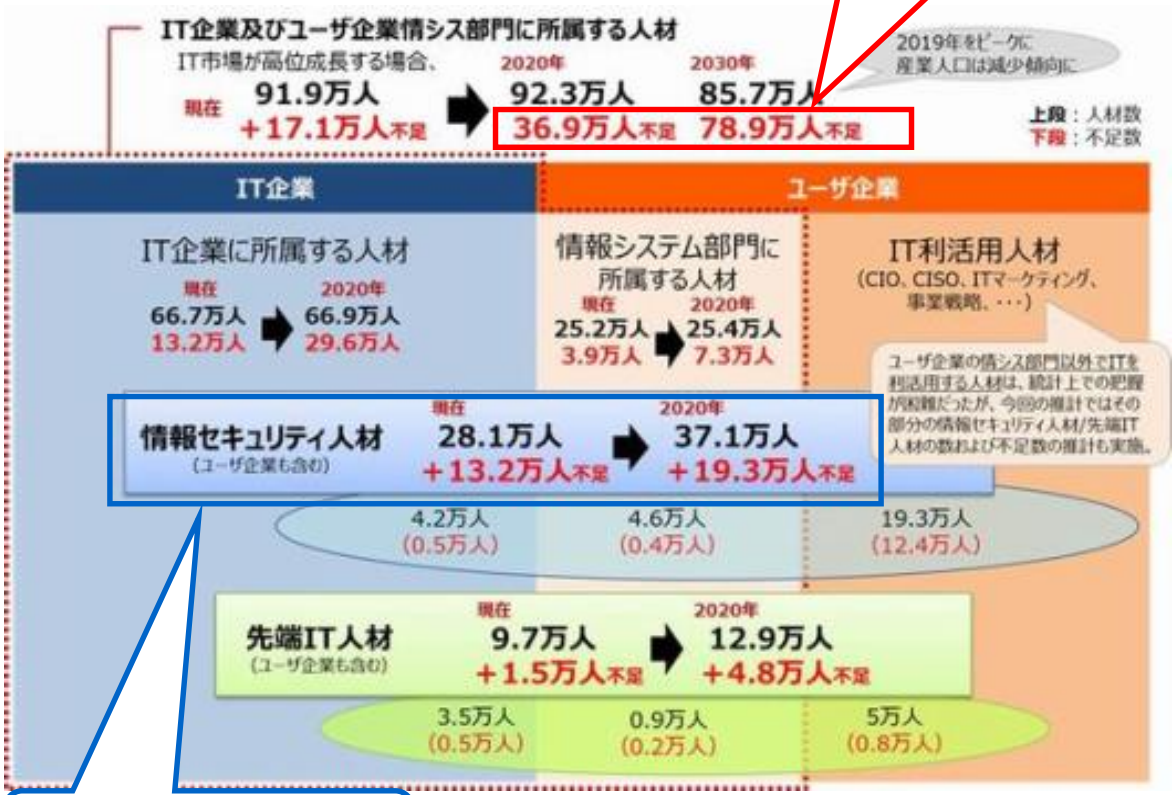
日本の強みであるリアルデータを核に、支援を強化

IT・データ・セキュリティ人材を巡る現状と将来

- IT人材は、**2030年には約79万人が不足する**と推定される
- AI・IoT・ビッグデータにより、**先端IT技術に関する市場は拡大する見込み**

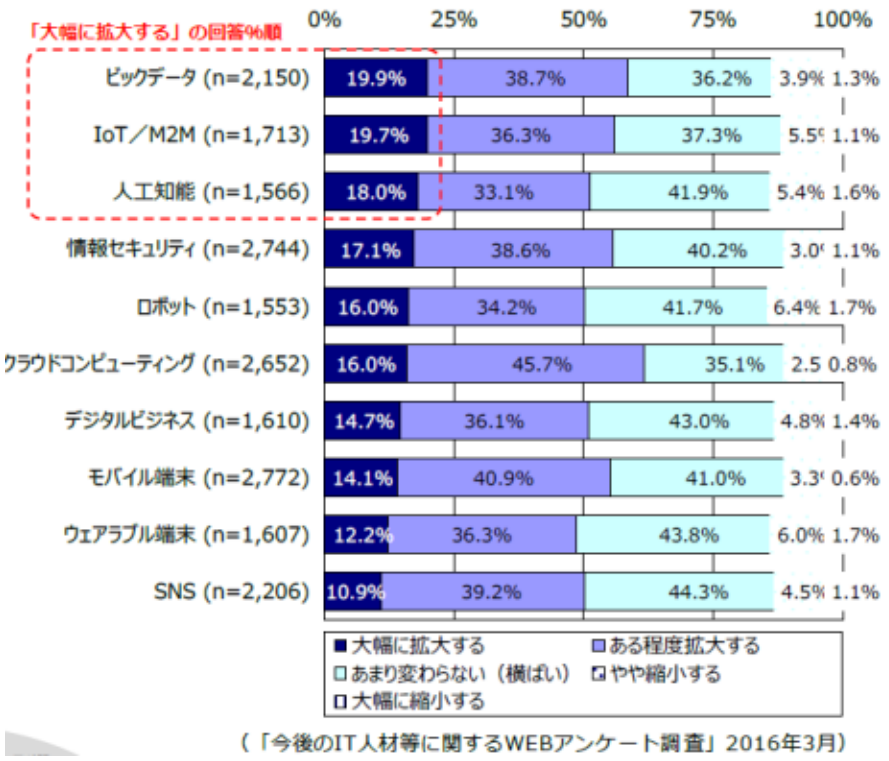
IT・データ人材の需給に関する推計

人材不足が深刻化するため、多様な人材の活用、スキルアップ支援による生産性の向上が急務



情報セキュリティ人材は、2020年で19.3万人不足。特にユーザー企業で大きな不足感

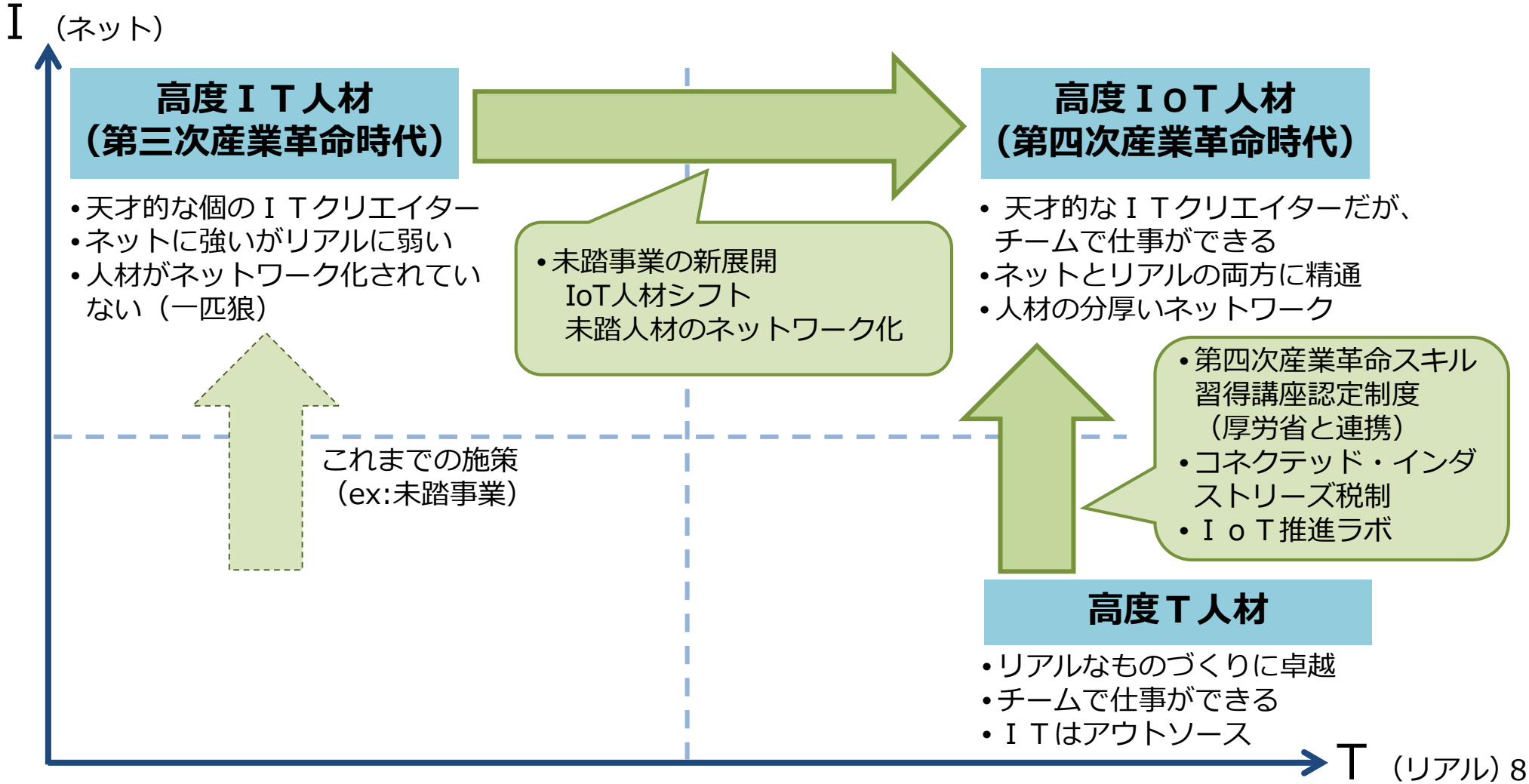
先端IT技術に関する今後の市場の拡大見込み



（「今後のIT人材等に関するWEBアンケート調査」2016年3月）

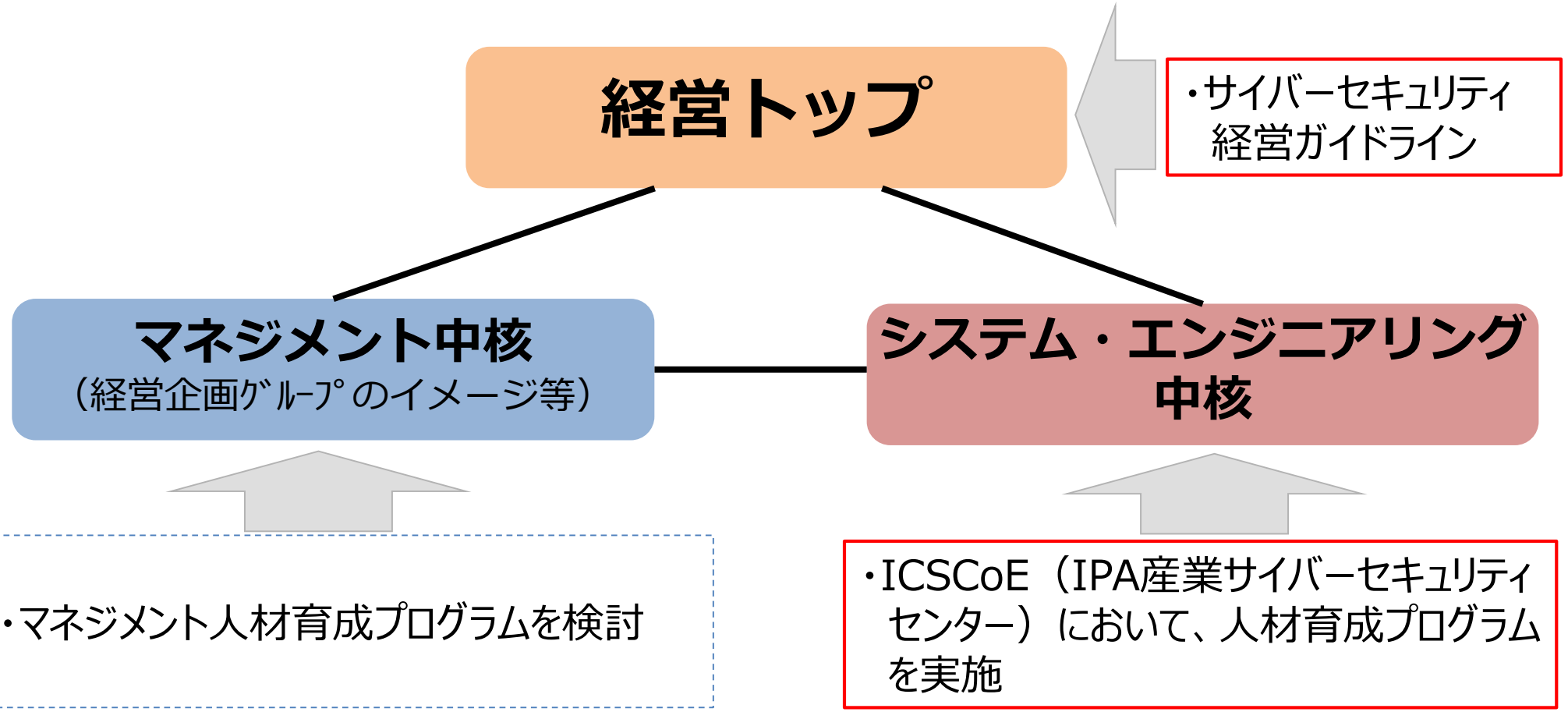
Connected Industriesの人材（高度ＩｏＴ人材）

- 天才的な個人がネット上ですべてを一変させ得た第３次産業革命は、終焉。
- 第４次産業革命は、ネットとリアルの双方に卓越し、チームで協業できる人材が必要。



サイバーセキュリティに対する人材育成の取組方針

- **サイバーセキュリティはビジネスリスク**であり、**それを理解して経営トップを支える人材の育成が鍵**。
- 特に求められる人材として、**ビジネスや技術を理解した上で、サイバーセキュリティのリスクを把握し、経営トップともコミュニケーションがとれるような、中核人材が重要**。



関 連 施 策

若手ＩＴ人材の育成（未踏ＩＴ人材発掘・育成事業）

- 未踏ＩＴ人材発掘・育成事業とは、いままで見たこともない「未踏的な」アイディア・技術をもつ「突出した人材」を発掘・育成する事業
- 25歳未満の天才的な個人が対象
- 産学界のトップで活躍する方を、プロジェクトマネージャー（PM）として登用し、PM独自の観点で天才を発掘・育成
- 開発費を支援し、PMの指導の下、9か月間の独創的なソフトウェア開発に挑戦（開発費上限230万円/件）

IPA 独立行政法人情報処理推進機構 Information-technology Promotion Agency, Japan

MITOU

2017年度未踏PM

竹内　郁雄　氏
東京大学名誉教授

夏野　剛　氏
慶應義塾大学
大学院
特別招聘教授

石黒　浩　氏
大阪大学
教授（特別教授）

竹迫　良範　氏
株式会社リクルート
マーケティング
パートナーズ
専門役員

首藤　一幸　氏
東京工業大学
准教授

藤井　彰人　氏
KDDI株式会社
本部長 兼 クラウド
サービス企画部長

五十嵐　悠紀　氏
明治大学
専任講師

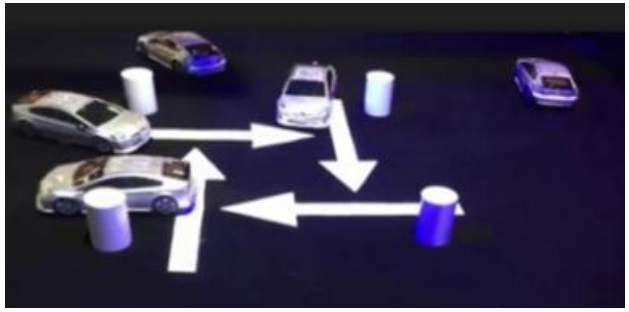
未踏卒業生による起業・事業化の事例

- 25歳未満の天才的な個人を対象
- これまでに、**1,680人の未踏IT人材を発掘・育成**。**約255名が起業・事業化**を行い、産業界の第一線で活躍
- ユニコーン候補となる**時価総額100億円以上の企業*も6社排出**

西川　徹氏
2005年度未踏採択
(株)プリファードインフラストラクチャー
代表取締役

ビッグデータをリアルタイムに処理する世界最高水準の技術を開発

自動運転等の実現に向けた、人工知能の研究開発に着手



落合 陽一氏
2009年度未踏採択
筑波大学助教
Pixie Dust Technologies .Inc
CEO

メディアアート作品の研究、制作により「現代の魔法使い」と呼ばれる

鈴木 健氏
2002年度未踏採択
スマートニュース(株)
代表取締役会長

ニュースキュレーションアプリの開発

福島 良典氏
2012年度未踏採択
(株)Gunosy創業者
代表取締役CEO

ニュースキュレーションアプリの開発

吉崎　航氏
2009年度未踏採択
(株)V-Sido代表

人型ロボット用のOSとも言える制御ソフトウェアV-Sidoを開発

＊プリファードインフラストラクチャー、トレジャーデータ、スマートニュース、グノシー、ブイキューブ、クラウドビーズ。

セキュリティ・キャンプ

- 高度複雑・高度化するサイバー攻撃に適切に対応するため、若年層のセキュリティ人材発掘の裾野を拡大し、世界に通用するトップクラス人材を創出することが必要。
- 民間企業と一丸となって、若年層セキュリティ人材の育成合宿を開催し、倫理面も含めたセキュリティ技術と、最新ノウハウを、第一線の技術者から伝授する場を創出。これまで累計で６６３名が受講した。また、地方におけるセキュリティ・キャンプ（地方大会）により、セキュリティ人材の裾野と輪を広げている。

セキュリティ・キャンプ卒業生の例

清水郁美さん
2015年修了（15歳）

毎年夏に、米国ラスベガスで開催される世界最大のハッカーの祭典「DEFCON(デフコン)。その目玉イベントのハッカー大会において、８位入賞を果たした。プログラミングや暗号解読をはじめとしたサイバーセキュリティ分野の技術力と知識を武器に、大人達に交じって勝ち抜き、セキュリティ・キャンプ修了生が有する高い技術力を発揮した。

情報処理安全確保支援士（登録セキスペ）制度

- 情報セキュリティの専門人材を確保できるよう、人材の識別を容易にするとともに、専門人材へのアクセスを確保するため、国家資格「情報処理安全確保支援士」（通称：登録セキスペ）制度を創設。

◆ 政府機関や企業等のサイバーセキュリティ対策を強化するため、専門人材を見える化し、活用できる環境を整備することが必要。

➡ **情報処理安全支援士の名称を有資格者に独占的に使用させることとし、さらに民間企業等が人材を活用できるよう登録簿を整備。**

◆ 技術進歩等が早いサイバーセキュリティ分野においては、知識等が陳腐化するおそれ。

➡ **有資格者の継続的な知識・技能の向上を図るため、講習の受講を義務化。義務に違反した者は登録を取り消される更新制を導入。**

◆ 民間企業等が安心して人材を活用できるようにするには、専門人材に厳格な秘密保持が確保されていることが必要。

➡ **業務上知り得た秘密の保持義務を措置。**

情報処理安全確保支援士（登録セキスペ）

2016年

10月21日　情報処理の促進に関する法律改正法施行

2017年

4月　1日　第1回登録により、4,172名の登録セキスペが誕生

4月16日　第1回試験実施（25,130名応募）

6月21日　第1回試験合格発表（2,822名合格）

10月　1日　第2回登録　新たに2,822名が登録

10月15日　第2回試験実施(23,452名応募)

12月20日　第2回試験合格発表（2,767名合格）

トピックス

◆コネクテッドインダストリー税制の計画認定時に登録セキスペ等によるセキュリティ確認を要件とする

◆政府情報システム調達ガイドラインにおいて、登録セキスペの関与例を明示。

情報処理安全確保支援士試験・情報処理技術者試験

- 「情報処理技術者試験」は、対象者別（IT利活用者・IT技術者）、レベル別（レベル１～４）に試験体系を構築。
- 平成29年度から、情報セキュリティスペシャリスト試験をベースとして「情報処理安全確保支援士試験」が開始
- 年間約45万人が応募する最大規模の国家試験（春と秋の２回実施）

情報セキュリティマネジメント試験（情報処理技術者試験）

- 今後必要となるセキュリティ人材のうち、ユーザー企業において、一定の技術知識を持ちつつ、自社内で情報セキュリティ対策の実務をリードできるマネジメント人材の評価の基準となる新試験として、情報処理技術者試験の中に新試験区分として「情報セキュリティマネジメント試験」を設け、平成28年春期から開始。2年間で合格者は49千人弱。

平成２８年度（春期・秋期）試験結果
応募者数：43,877人
合格者数：28,905人

平成２９年度（春期・秋期）試験結果
応募者数：42,069人
合格者数：19,914人

第四次産業革命スキル習得講座認定制度（概要）

Reスキル講座

● ＩＴ・データを中心とした将来の成長が強く見込まれ、雇用創出に貢献する分野において、社会人が高度な専門性を身に付けキャリアアップを図る、専門的・実践的な教育訓練講座を経済産業大臣が認定する。

※ 厚生労働省が定める一定の要件を満たし、厚生労働大臣の指定を受けた講座は「専門実践教育訓練給付」の対象となる。

■講座の要件

- ✓ 育成する職業、能力・スキル、訓練の内容を公表
- ✓ 必要な実務知識、技術、技能を公表
- ✓ 実習、実技、演習又は発表などが含まれる実践的な講座がカリキュラムの半分以上
- ✓ 審査、試験等により訓練の成果を評価
- ✓ 社会人が受けやすい工夫（e-ラーニング等）
- ✓ 事後評価の仕組みを構築　等

■実施機関の要件

- ✓ 継続的・安定的に遂行できること（講座の実績・財務状況等）
- ✓ 組織体制や設備、講師等を有すること
- ✓ 欠格要件等に該当しないこと　等

■認定の期間

- ✓ 適用の日から３年間

■対象分野・目標

※IT技術の基礎・初級は対象としない。

(1) IT（IT業界）

新技術・システム	①	クラウド、ＩｏＴ、ＡＩ、データサイエンス　等 開発手法：デジタルビジネス開発（デザイン思考、サービス企画、データ分析、アジャイル等）との組み合わせも想定
高度技術	②	ネットワーク、セキュリティ　等

(2) 産業界のＩＴ利活用

自動車（モデルベース開発）　等

（目標）

ＩＴＳＳレベル４相当を目指す

※ ＩＰＡ等からの専門的な助言を踏まえ、外部専門家による審査を経て認定を行う

（参考）第四次産業革命スキル習得講座（第１回認定）

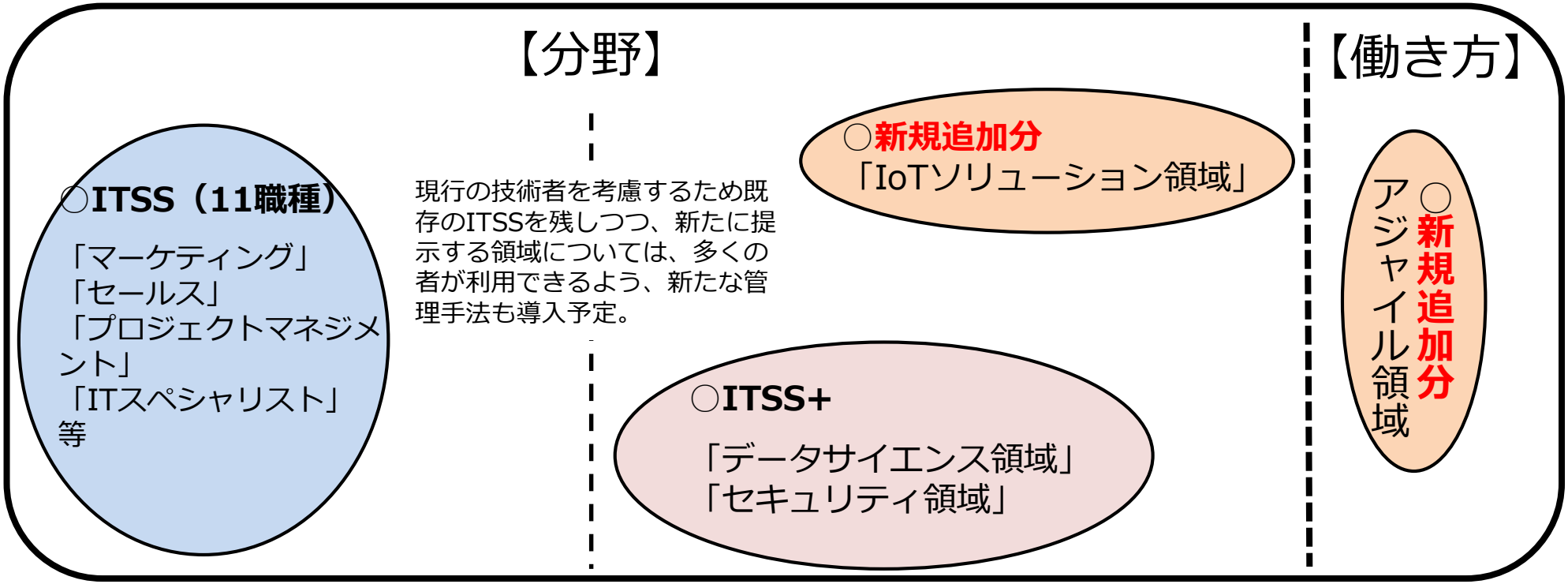
Reスキル講座

ＡＩ（４講座）	
株式会社チェンジ	「AI活用コンサルタント」育成トレーニング　～AIer 育成プログラム～
株式会社ウチダ人材開発センタ	ＡＩ活用講座
日本マイクロソフト株式会社	ディープラーニングハンズオンセミナー
株式会社富士通ラーニングメディア	Fujitsu Digital Business College／AI・データ分析を活用するイノベーター
ＩｏＴ（１講座）	
株式会社ウチダ人材開発センタ	ＩｏＴ活用講座　上級編
クラウド（４講座）	
デジタルハリウッド株式会社	ジーズアカデミーTOKYO　LABコース
NECマネジメントパートナー株式会社	クラウド基盤構築とクラウドサービス適用検討 -Microsoft Azure編-
株式会社ITプレナーズジャパン・アジアパシフィック	ICT利活用コース　～クラウドサービスマネジメント～
株式会社富士通ラーニングメディア	デジタルビジネス創出人材育成コース
データサイエンス（７講座）	
株式会社ｅｆｔａｘ	データ分析教育講座　白・茶・黒帯編
株式会社ブレインパッド	データサイエンティスト入門研修
株式会社ブレインパッド	データサイエンティスト入門研修（アドバンスド）
株式会社アイ・ラーニング	データサイエンティスト育成講座
株式会社チェンジ	データサイエンティスト養成コース
株式会社日立インフォメーションアカデミー	データ利活用技術者育成講座
フューチャー株式会社	データサイエンティスト養成講座
セキュリティ（６講座）	
株式会社アイ・ラーニング	日本IBM　CSIRT研修
NECマネジメントパートナー株式会社	情報セキュリティ技術者養成講座
シーティーシー・テクノロジー株式会社	セキュリティエンジニア養成講座
株式会社ラック	実践！デジタル・フォレンジック完全マスター
株式会社ラック	実践！マルウェア解析完全マスター
ネットワンシステムズ株式会社	CSIRT能力向上研修
自動車（モデルベース開発）（１講座）	
公益財団法人ひろしま産業振興機構	モデルベース開発プロセス研修

ITスキル標準の見直しについて

- 情報サービスの提供に必要な実務能力を明確化・体系化したITスキル標準(ITSS)に加え、本年4月に「データサイエンス領域」及び「セキュリティ領域」を追加したITSS＋を公表。さらに、本年度末までに、「アジャイル領域」及び「IoTソリューション領域」の追加を予定。
- 今後、技術トレンドの早い変化に対応して、随時ITスキル標準の領域の追加を行っていく。

【新ITSSの全体像】

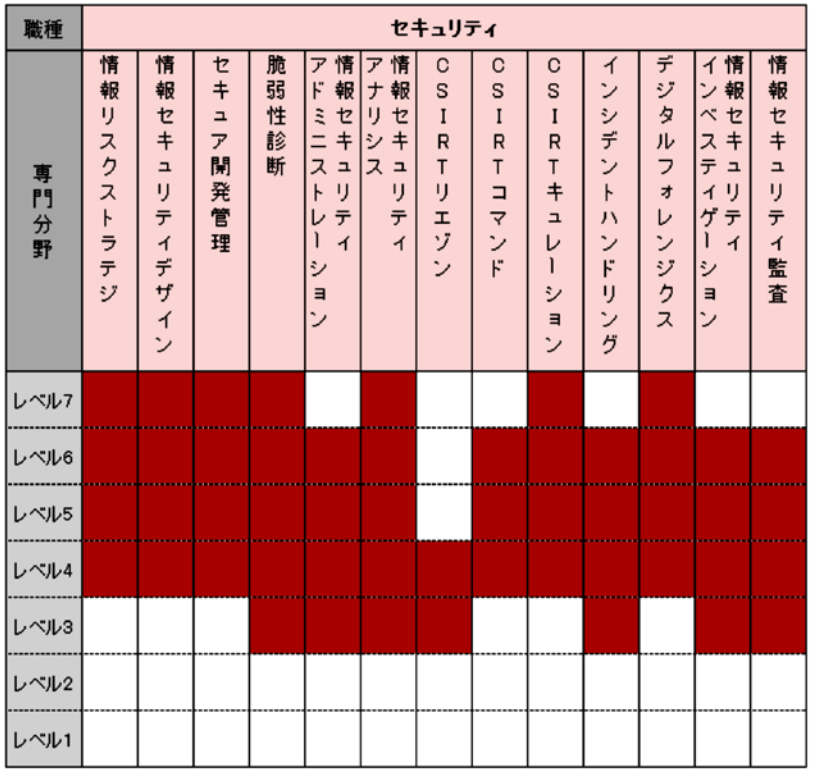


（参考）ITSS＋について（セキュリティ領域）

- ITSS+は、キャリアフレームワークとして、ビジネスの実状に沿うように専門分野を分類定義し、IT技術者個人の能力や実績のレベルに対して個人のスキルを評価する尺度を提供。セキュリティやデータサイエンス分野における企業内の「タスク（業務）」と、それを担うべき「専門人材」や「スキル」の把握、人材育成計画の立案、研修プログラムの開発を効率的に進めることが可能となる。
- 今後、セキュリティやデータサイエンス分野の専門家だけでなく、より多くの研修事業者や教育機関等においてIT人材育成の取組みが活発に行われるよう、各レベル毎に求められるスキルの達成方法がIT専門家以外の者にも理解しやすい内容としていく予定。

＜セキュリティ領域の例＞

■キャリア・フレームワーク



■専門分野の説明

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に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。
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に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システム的な鑑識、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。

サイバーセキュリティ経営ガイドライン（平成27年12月28日公開、平成29年11月16日改訂）

- 経済産業省と（独）情報処理推進機構（IPA）にて策定。
- 経営者のリーダーシップによってサイバーセキュリティ対策を推進するため、**経営者が認識すべき3原則**と、**経営者がセキュリティの担当幹部（CISO等)に指示すべき重要10項目**を提示。

1．経営者が認識すべき３原則

（1）経営者は、サイバーセキュリティリスクを認識し、**リーダーシップによって対策を進める**ことが必要

（2）自社は勿論のこと、ビジネスパートナーや委託先も含めた**サプライチェーンに対するセキュリティ対策が必要**

（3）平時及び緊急時のいずれにおいても、サイバーセキュリティリスクや対策に係る情報開示など、**関係者との適切なコミュニケーションが必要**

2．経営者がCISO等に指示すべき１０の重要事項

リスク管理体制の構築

（指示１）サイバーセキュリティリスクの認識、組織全体での対応方針の策定
（指示２）サイバーセキュリティリスク管理体制の構築
（指示３）サイバーセキュリティ対策のための資源（予算、人材等）確保

インシデントに備えた体制構築

（指示７）**インシデント発生時の緊急対応体制の整備**
（指示８）**インシデントによる被害に備えた復旧体制の整備**

リスクの特定と対策の実装

（指示４）サイバーセキュリティリスクの把握とリスク対応に関する計画の策定
（指示５）**サイバーセキュリティリスクに対応するための仕組みの構築**
（指示６）サイバーセキュリティ対策におけるPDCAサイクルの実施

サプライチェーンセキュリティ

（指示９）**ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握**

関係者とのコミュニケーション

（指示10）情報共有活動への参加を通じた攻撃情報の入手とその有効活用及び提供

※赤字及び太字は平成29年度11月16日改訂部分

重要インフラ・産業基盤のサイバーセキュリティ対策を担う人材の育成

- 2017年4月、IPAに産業サイバーセキュリティセンター(Industrial Cyber Security Center of Excellence, ICSCoE)を設置。電力、ガス、鉄鋼、石油、化学、自動車、鉄道、ビル、空港、放送、通信、住宅等の各業界60社以上から約80名の研修生を受け入れ、実践的な演習・対策立案等のトレーニングを行う。
- 2017年9月、米国・国土安全保障省（DHS）及びICS-CERTから専門家を招聘し、「産業分野におけるサイバーセキュリティの日米共同演習」を実施。
- 2017年11月、イスラエルから複数の有識者を招聘し、世界の最新動向を踏まえた特別講義の開催。

IT系・制御系に精通した専門人材の育成

模擬プラントを用いた対策立案

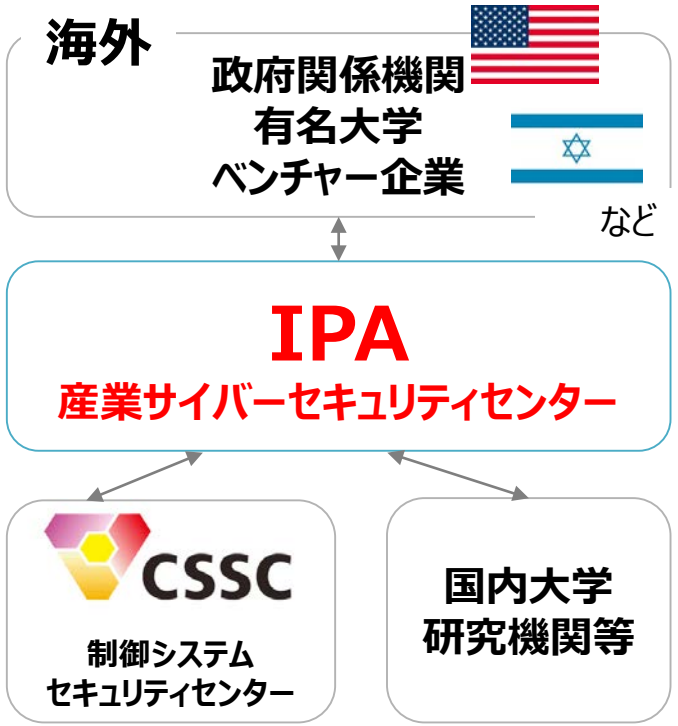
- 情報系システムから制御系システムまでを想定した模擬プラントを設置。専門家とともに安全性・信頼性の検証や早期復旧の演習を行う。
- 海外との連携も積極的に実施。

実際の制御システムの安全性・信頼性検証等

- ユーザーからの依頼に基づき、実際の制御システムやIoT機器の安全性・信頼性を検証。
- あらゆる攻撃可能性を検証し、必要な対策立案を行う。

攻撃情報の調査・分析

- おとりシステムの観察や民間専門機関が持つ攻撃情報を収集。新たな攻撃手法等を調査・分析。



ＩｏＴ投資の抜本強化（コネクテッド・インダストリーズ税制の創設）

新設

（所得税・法人税・法人住民税・事業税）

- **一定のサイバーセキュリティ対策**が講じられた**データ連携・利活用**により、**生産性を向上させる取組**について、それに必要となる**システムや、センサー・ロボット等の導入**に対して、**特別償却30%又は税額控除3%（賃上げを伴う場合は5%）**を措置。
- 事業者は当該取組内容に関する**事業計画を作成**し、**主務大臣が認定**。**認定計画に含まれる設備に対して、税制措置を適用（適用期限は、平成32年度末まで）。**

【計画認定の要件】

①データ連携・利活用の内容

・社外データやこれまで取得したことのないデータを社内データと連携

・企業の競争力における重要データをグループ企業間や事業所間で連携

②セキュリティ面

必要なセキュリティ対策が講じられていることをセキュリティの専門家(登録セキスペ等)が担保

③生産性向上目標

投資年度から一定期間において、以下のいずれも達成見込みがあること

・労働生産性：年平均伸率２%以上

・投資利益率：年平均15%以上

課税の特例の内容

➢ 認定された事業計画に基づいて行う設備投資について、以下の措置を講じる。

対象設備	特別償却	税額控除
ソフトウェア 器具備品 機械装置	30%	3% （法人税額の15%を限度） 5％ ※ （法人税額の20%を限度）

【対象設備の例】

データ収集機器（センサー等）、データ分析により自動化するロボット・工作機械、データ連携・分析に必要なシステム（サーバ、ＡＩ、ソフトウェア等）、サイバーセキュリティ対策製品　　等

最低投資合計額：5,000万円

※ 計画の認定に加え、平均給与等支給額の対前年度増加率≧３%を満たした場合。