サイバーセキュリティ人材育成総合強化方針
（案）

平成 28 年　月　　日
普及啓発・人材育成専門調査会

はじめに

平成 27 年9月、「サイバーセキュリティ戦略」（以下「戦略」という。）を閣議決定した。戦略は、「自由、公正かつ安全なサイバー空間」を創出するため、3つの政策分野（「経済社会の活力の向上及び持続的発展」、「国民が安全で安心して暮らせる社会の実現」、「国際社会の平和・安定及び我が国の安全保障」）と1つの分野横断的施策（研究開発や人材育成を含む基礎体力の強化）で構成されており、各施策を着実に推進していく必要がある。

サイバー空間は、その大部分が民間設備投資で成り立っている人工空間であり、あらゆるモノがネットワークに接続され、実空間とサイバー空間との融合が高度に深化した「連接融合情報社会」が到来しつつある中、経済社会の発展、その基礎となるサイバー空間の安全確保の実現のためにも民間分野の積極的な投資が重要である。このため、サイバーセキュリティ関連産業を振興し、民間投資が進む環境を整備することが必要である。同時に、行政分野においても、サイバー空間上の脅威への対処等に係る政策を適切に立案し、実施していくための体制整備が必要となる。

こうした課題を解決するためには、量的・質的に不足しているサイバーセキュリティ人材の育成が急務である。この取組は、平成 32 年に開催される 2020 年東京オリンピック・パラリンピック競技大会を成功裏に導くためにも不可欠である。このため、平成 28 年度以降の人材育成に係る各種施策を強化するとともに、各施策の円滑な連携を促進するため、「サイバーセキュリティ人材育成総合強化方針」を取りまとめた。本方針は、社会で活躍できる人材の育成に向け、サイバーセキュリティを専門とする人材のみならず、ユーザー企業等も含めた幅広い立場でのサイバーセキュリティに係る人材育成に向けた各種施策を加速させていくための方針を示す。

Ⅰ　社会で活躍できる人材の育成

1. 人材の需要と供給の好循環の形成

あらゆるモノがネットワークに接続され、実空間とサイバー空間との融合が高度に深化した「連接融合情報社会」が到来しつつあり、安全な製品・サービスの実現・提供が国・企業としての競争力の源泉となっている。こうした社会では、各種の製品・サービスの企画から実利用に至る様々な段階においてセキュリティの知識を駆使できることが必要となる。このことは、IT[1]ベンダーやセキュリティベンダーのみならず、ユーザー企業や政府機関においても該当するものである。今後、新ビジネスの創出や既存ビジネスの高度化を実現していくためには、必要となるサイバーセキュリティに係る人材の確保が可能となる社会的な仕組みづくりや具体的な取組の推進が急務となっている。

こうした認識の下、経営層においては、サイバーセキュリティに係る取組が経営戦略における不可欠な事業であることを認識し、その推進のために必要な人材を確保し、これらの人材が活躍できるキャリアパスを実現していくことが求められる(「人材の需要」)。また、人材の需要に応えるためには、確かな知識と実践力を備え、様々な業務経験を積み重ね、必要に応じて新たな知識や実践力を習得し、さらにその能力を向上させていく人材を育成するための仕組みや取組が求められる(「人材の供給」)。そして、このような「人材の需要(雇用)」と「人材の供給(教育)」を相応させ、好循環の形成を促進することが求められる。このため、人材育成に係る施策の検討・推進に際しては、産学官の連携体制によって、進めることを基本とする。

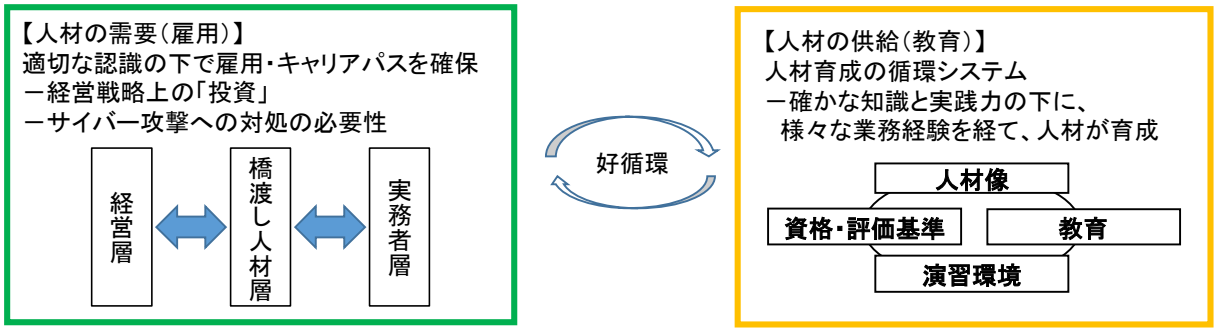

図1:サイバーセキュリティ人材育成に係る需要と供給の好循環(概念図)

2. 経済社会の変化に対応した経営戦略

戦略ではサイバーセキュリティの取組を「投資」と認識すべきとしており、この観点から戦略的に事業を行っていく人材が「経営層」、「橋渡し人材層」、「実務者層」の各層において求められ

1 情報通信技術(Information Technology)の略称

る。具体的には、「経営層」において、サイバーセキュリティに係る取組を経営戦略の一環として積極的に取り組むよう意識改革を促す。そして、経営層と実務者層との間のコミュニケーションを円滑にする「橋渡し人材層」の育成を推進するとともに、「実務者層」において、産学官連携した人材育成の循環システムを構築し、その充実を促進する。

（1）「経営層」の意識改革（人材の需要の喚起）

・サイバーセキュリティ対策を実施するための経営ガイドラインの普及を促進する。（継続）
・企業価値を高めるサイバーセキュリティ投資の取組に係る、情報発信の在り方等について取りまとめる。（平成 28 年6月を目途）

連接融合情報社会においては、安全な製品・サービスを提供するセキュリティ品質が企業価値や国際競争力の源泉となる。こうした社会の変化をより多くの企業経営層が的確に捉え、セキュリティ対策はやむを得ない「費用」ではなく、より積極的な経営への「投資」であるとの認識を醸成していくことが重要である。このため、サイバーセキュリティに関する取組が、市場や出資者といったステークホルダーから正当に評価されるための方策について取り組む。

具体的には、企業の経営者を対象に、経営者のリーダーシップの下で、サイバーセキュリティ対策を推進するため、サイバー攻撃から企業を守る観点で、経営者が認識する必要のある「3原則」、及び経営者が情報セキュリティ対策を実施する上での責任者となる担当幹部（CISO[2]等）に指示すべき「重要 10 項目」をまとめた「サイバーセキュリティ経営ガイドライン」[3]の普及について、説明会やセミナー等を活用しつつ推進する。

また、今後、安全なIoT[4]システムを活用した新規事業や既存ビジネスの高度化に伴い、サイバーセキュリティの確保がユーザーから求められることから、企業等がサイバーセキュリティ対策に取り組んでいることをステークホルダー等に情報発信する方策等について検討し、その結果を平成 28 年6月を目途に取りまとめる。

2 Chief Information Security Officer の略称
3 経済産業省、平成 27 年 12 月公表
4 Internet of Things の略称

（2）「橋渡し人材層」の育成

・経営層と実務者層との間のコミュニケーションを取りやすくするためのツールとしての具体的な事例を交えたコンテンツを作成する。（平成 28 年6月を目途）
・組織内をまとめ、指揮できる能力を高めるため、組織横断的な調整、マネジメント能力を目的とした演習を実施する。（継続・拡充）
・サイバーセキュリティと経営等の他分野との専門を併せ持つ教育を推進する。（継続）

サイバーセキュリティの考え方や能力を、企業経営において使いこなすためには、経営層と実務者層の双方が、サイバーセキュリティに関する課題や解決の方向性を共有する必要がある。しかしながら、経営層が直接、サイバーセキュリティの専門的な知見を有する実務者層一人一人とコミュニケーションをとっていくことは難しい。このため、経営層の示す経営方針を理解し、サイバーセキュリティに係るビジョンの提示や、実務者層との間のコミュニケーションの支援を行う橋渡し人材層が必要であり、その育成を推進する。

橋渡し人材層は、経営層の示す経営方針に基づくサイバーセキュリティ対策を実践すること、実務課題を踏まえた経営戦略を提示すること、さらに、実務者層をまとめ、リードすることができることが必要である。

また、橋渡し人材層は、単にサイバーセキュリティの知識を有するだけでなく、実務面からくる技術的なものを含めサイバーセキュリティに係る課題について、提供する機能やサービスを全うするという観点からリスクを分析し、残存リスクの情報も添えて経営者層に対し提供し総合的な判断を受ける「機能保証（任務保証）」の考え方に基づく取組が求められる。さらに、経営の立場や危機管理上の課題からも、どのようなサイバーセキュリティ対策を取るべきかを示すことが求められるため、実際に実務者として組織内の業務経験を積む必要があり、実務者層をまとめ指揮できるリーダー的な役割を担うことが期待される。

そのため、経営層と実務者層との間のコミュニケーションの支援を行う橋渡し人材層が経営層に対し、サイバーセキュリティに係るビジョンの提示等の際にコミュニケーションを取りやすくするためのツールとして、具体的な事例を交えたコンテンツを平成 28 年6月を目途に作成する。

また、これまで、主に実務者層の技術者向けに行ってきたサイバーセキュリティに係る演習において、対外公表や組織内の対応方針の決定等、マネジメント能力を高めるための演習を行うことにより、「橋渡し人材層」の能力向上を図る。

加えて、例えば、一定のサイバーセキュリティに係る業務を含めて勤務経験の後、大学院等の

教育機関でサイバーセキュリティのみならず、経営や法律等の他分野の専門知識を身に付ける集中的かつ体系的な学習の機会が与えられる、リカレント教育の充実等の橋渡し人材層の育成に向けた取組を促進する。

3. 産学官が連携した人材育成の循環システムの構築

これまで、サイバーセキュリティ人材の育成に関しては、産学官それぞれが取り組んできているものの、各取組間の関係については十分に連携した役割分担の下で進められてきたとは言い難い。

このため、ユーザー企業等も含めサイバーセキュリティの知識を駆使できることが広く求められているという、その社会的ニーズに見合ったサイバーセキュリティ人材の育成に向け、求められる人材像を明示し、その人材像の実現に向け、理論・基礎の習得のための産学官が連携した教育、実際にサイバーセキュリティ対策を行う実務者層の実践力の強化のための演習環境の整備、サイバーセキュリティに従事する者の能力の可視化に資する資格・評価基準の整備、一旦就職した後に、技術的能力や他分野の能力を高めるリカレント教育といった各取組が、人材育成の循環システムとして形成されることを目指す。その際、確かな知識と実践力の下に、様々な業務経験を積み重ねて人材が育成されるよう産学官が密接に連携する。加えて、グローバルかつ高度なサイバー攻撃等に対応し、サイバーセキュリティに係る突出した能力を有した人材の発掘・確保にも努める。

これらの取組を実施するにあたっては、学校教育のみならず、企業内においても産業横断的な育成プログラムの活用やインターンシップ等の人材育成プログラムが充実されることが重要である。

（1）求められる人材像の明示

・組織の性質・組織の構成毎に求められるサイバーセキュリティに係る人材像を明確化する。（平成 28 年度中を目途）

サイバーセキュリティ人材の育成に当たっては、まず、「求められる人材像」を明確にすることが必要である。IT 製品・サービスのベンダー側の立場のみならず、ユーザー側の立場の双方において、「実務者層」、「橋渡し人材層」ごとに求められる人材像は異なってくると考えられる[5]。例えば、ユーザー側の立場においては、その業務において、どのようなセキュリティ対策が必要である

5 「新・情報セキュリティ人材育成プログラム」（平成 26 年5月情報セキュリティ政策会議決定）9頁参照

かを認識した上で、経営層の示す経営方針を理解し、サイバーセキュリティに係るビジョンの提示や、実務者層との間のコミュニケーションの支援を行うことができる橋渡し人材層が求められる。このような人材には、サイバーセキュリティの知識だけでなく、経営等他分野の知識を併せ持つ「ハイブリッド型人材」が求められる。また、突出した人材はベンダー側の立場の実務者層などにおいても求められる。

こうした中、産業界においても業種・業界毎に求められる人材像の明確化等を目標として検討する動きがあり[6]、そうした動向も踏まえつつ、人材育成施策において目標とする人材像を明確化し、平成 28 年度中にまとめる。その上で、その人材像にかなう人材を育成するにあたり、産学官が連携した教育の充実、演習環境の整備、資格・評価基準等の能力の可視化、突出した人材の発掘・確保の各種施策を推進していく。これら4つの施策の具体的な取組方針について次節以降に述べる。

（2）産学官が連携した教育の充実

・社会の変化に柔軟に対応していくことができる基礎的な教育の充実と、社会のニーズを踏まえた教育を産学官連携して推進する。（継続・拡充）
・大学等の教育プログラムと、各種試験・資格との連携、関連づけ等に関する検討を進める。

サイバーセキュリティに関する素養は、すべての人にとって必要なものとなりつつある中、理論・基礎の習得について大学等の段階から行われることが期待される。その際、社会の変化に柔軟に対応していくことができる基礎的な教育の充実と、社会のニーズ、求められる人材像に合致した教育の実施が求められる。

企業からの寄附講座の開設や講師派遣等が進みつつあるが、さらに、産業界と連携した教育プログラムの開発等を行い、地域における教育機関なども含め、共有化することが重要となる。また、橋渡し人材層の育成のため、専門性を深めるとともに、他分野の知識を併せ持つハイブリッド型人材を育成するための大学間連携、リカレント教育の充実等の促進も求められる。

このため、これらの連携実現に向けた取組として、

6 平成 27 年6月、複数の企業関係者が集まり、「産業横断サイバーセキュリティ人材育成検討会」が発足した。そこでは、人材育成は社会的価値の創出（社会的課題の解決）と捉え、産々連携も視野に入れた検討が進められている。平成 28 年1月に公開された中間報告では、「セキュリティ業務は企業組織内で広範に分散しており、セキュリティ専門組織の人材育成だけでは不十分であること」や「ユーザー企業としてセキュリティ人材を育成または採用し、企業として活用・維持し続けることが可能な仕組みが必須であり、そのための産学官連携の在り方の議論が急務であること」といった課題が示されている。

・高等専門学校において、企業等と連携した情報セキュリティのスキルセット（到達目標）の構築、教材開発、実践的な演習環境の整備等の実施（平成 28 年度より実施）

・大学・大学院において、大学間連携によって、技術系科目と社会科学系科目を併せて学ぶハイブリッド型人材の育成強化、産学の教育ネットワークの構築を図る「成長分野を支える情報技術人材の育成拠点の形成」（enPiT[7]）等の実施（大学学部については、平成 28 年度より実施）

・大学等における社会人や企業等のニーズに応じた実践的・専門的なプログラムを国が認定する「職業実践力育成プログラム（BP[8]）」制度等の活用により、社会人の学び直しの促進（継続）

・専門学校において企業等との密接な連携を行う学科を文部科学大臣が認定する「職業実践専門課程」等により、産学連携による取組を実施。（継続）

などについて、取組の効果等について検証しつつ必要に応じて改善・推進を図る。

さらに、大学等における教育プログラムを受けることによって、どのくらいの知識・能力が身に付くかについて明らかにするために、大学等の教育プログラムと各種IT・セキュリティに係る試験・資格との連携、関連づけ等に関する検討を進める。

（3）演習環境の整備

・社会のニーズを踏まえた、実践的なサイバーセキュリティの演習を強化するとともに、その環境を整備する。（継続・拡充）
・技術的な内容のみでなく、組織横断的な調整能力やマネジメント等についても向上させる演習を実施する。（平成 28 年度以降）

サイバーセキュリティに係る知識を実際に活用できるためには、実践力を身に付けることが重要であり、そのための演習の取組を強化するとともに、実践的なサイバーセキュリティの演習環境を整備する。

これまでも国立研究開発法人情報通信研究機構（NICT[9]）が有する演習基盤を活用して、主に国の行政機関、地方自治体、重要インフラ事業者等[10]の LAN[11]管理者のサイバー攻撃への対

7 Education Network for Practical Information Technologies の略称
8 Brush up Program for professional の略称
9 National Institute of Information and Communications Technology の略称
10情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス（地方公共団体を含む）、医療、水道、物流、化学、クレジット及び石油の 13 分野。
11 Local Area Network の略称

応能力向上のため、実践的なサイバー防御演習（CYDER[12]）を実施してきたところである。この取組を一層強化するため、NICTが、サイバーセキュリティに関する技術的知見や研究成果等を活かした実践的な演習及び関連する教育コンテンツの制作等を実施することとし、NICT の業務に当該演習に係る業務を追加するための法整備を行う。（平成 28 年度より実施予定）

この際、サイバー攻撃への実践的な対処能力としては、個別のサイバー攻撃への技術的な対処能力だけでなく、組織横断的な調整能力や発生した事態に対するマネジメント能力等も求められることとなる。また、平成 28 年度以降の演習は、国の行政機関、地方自治体、独立行政法人、重要インフラ事業者等、対象を大幅に拡大して実施することとする。なお、こうした演習については、産業界や大学等からのニーズを踏まえ、産学官連携で演習環境の充実に向けた検討を進める。

また、特に対策が求められる重要インフラ事業者を対象として、計装事業者などが有する制御システムセキュリティの知見を高めるため、技術研究組合制御システムセキュリティセンター（CSSC[13]）のテストベッドを活用し、制御システムにおけるサイバーセキュリティ演習を引き続き実施するとともに、高度なスキルを持った人材がさらなる高見を目指せるような演習も拡充・実施していく。

さらに、国立大学法人等の情報セキュリティ担当者に対し、サイバー攻撃への対処能力の向上を図るために、大学共同利用機関法人情報・システム研究機構国立情報学研究所が実践的な演習環境を整備していく。（平成 28 年度より実施）

（4） 資格・評価基準等の能力の可視化

・産業界や大学等社会で活用される資格・評価基準等を整備する。（継続・拡充）
・サイバーセキュリティに従事する者の実践的な能力を適時適切に評価できる資格制度を整備する。（平成 28 年度中）
・IT を利活用する技術者等がサイバーセキュリティに関する知識や技能を習得することをめざし、必要なスキルを取りまとめる。（平成 28 年度中）

大学等で習得した知識や、演習や業務経験で身に着けた実践力を評価し、組織内での業務・処遇に反映させるとともに、さらなる能力の向上に向けた自己研鑽の機会とするため、サイバーセキュリティに関する能力を可視化するための試験制度、資格を整備していくことが重要である。

12 CYber Defense Exercise with Recurrence の略称
13 Control System Security Center の略称

このため、最新のサイバーセキュリティに関する知識・技能を備えた、高度かつ実践的な人材に関する国家資格である「情報処理安全確保支援士」の創設に係る取組を進め、平成32年度までに3万人の有資格者の確保を目指す。本制度においては、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するとともに、情報処理安全確保支援士の名称を有資格者に独占的に使用させることとする。また、民間企業等が人材を活用できるよう登録簿を整備することとし、本制度の創設に係る法改正案の国会での審議を経て具体的な制度内容を平成 28 年中に取りまとめる。

また、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たな試験として「情報セキュリティマネジメント試験」を、平成 28 年春期から情報処理技術者試験の一部として導入したところであり、その普及を図る。

前述のように、組織において必要となるサイバーセキュリティに係る能力として、サイバー攻撃への対処等の技術的な能力と、組織内でサイバーセキュリティ対策の実務の体制を整備するマネジメントの能力に大きく分けられるが、組織においてはその双方の立場の人材が連携してサイバーセキュリティ対策を進めていく必要がある。このような能力が適切に評価されるには、具体的な制度設計や運用が重要であることから、資格等の制度設計にあたっては、利用者である産業界や大学等の多様なステークホルダーからのニーズを踏まえたものとする。

さらに、今後、企画設計の段階からサイバーセキュリティを考慮した安全な IT システムが求められることから、IT を利活用する技術者等がサイバーセキュリティに関する知識や技能を習得することをめざし、独立行政法人情報処理推進機構（IPA）[14]が整備する IT スキル標準の中に必要なスキルを取りまとめ、その普及を促進する。（平成 28 年度中）

加えて、能力を可視化した上で、能力に見合った適正な処遇を実現していくことも重要であり、産学官が連携して適性処遇の推進やキャリアパス等の整備を検討していく。

（5）突出した能力を有した人材の発掘・確保

・グローバル水準の能力を競うコンテスト等を通じて人材を発掘・確保する。（継続）
・セキュリティキャンプ等、突出した能力を持ちうる人材が切磋琢磨できる環境を整備する。（継続）

サイバーセキュリティの分野は急激に変化し続けており、日々発生する新たな事案、高度な事

14 Information-technology Promotion Agency の略称

案への対処には、環境の変化に対応した新たな対策を創ることができる高度な専門性及び突出した能力を有する人材の確保が不可欠である。また、サイバーセキュリティがグローバルな課題となっていることに鑑みれば、こうした突出した能力を有する人材はグローバル水準の能力を備える必要がある。

このため、若年層のセキュリティ人材の裾野を拡大し、世界に通用するトップクラス人材の創出を目的とした、「セキュリティキャンプ」や「未踏IT人材発掘・育成事業」のような挑戦の機会を設けることによって、突出した能力を持ちうる人材を発掘することができる“場”づくりを実施する。また、将来活躍が期待される意欲と能力のある学生を顕彰するなどの支援を行う。

また、博士課程を中心に企業や組織での業務経験を有する者に対し、リアルなサイバー攻撃データも活用し、攻撃の状況を俯瞰・判断するシミュレーション演習等を実施し高度人材の育成を行う（平成 28 年度より実施）。

加えて、2020 年東京オリンピック・パラリンピック競技大会を見据え、本大会関連システムの模擬も可能な大規模演習基盤を構築・運用し、より高度な専門性を有するサイバーセキュリティ人材の育成に対する支援を実施していく（平成 28 年度より実施）。

また、グローバル水準の人材育成においては、海外の人材登用や海外への人材派遣などを深めることによって、サイバー攻撃への対策に対する実践的な能力を身につけることが期待できる。そのために、突出した能力を持つ人材が海外のハイレベルなコンテストや演習に参加することを促すことや、我が国に海外の有能な人材が魅力を感じられるような場（国際的なコンテストや実践的な演習環境）を整備していくとともに、民間団体における同種の取組を積極的に支援していく。

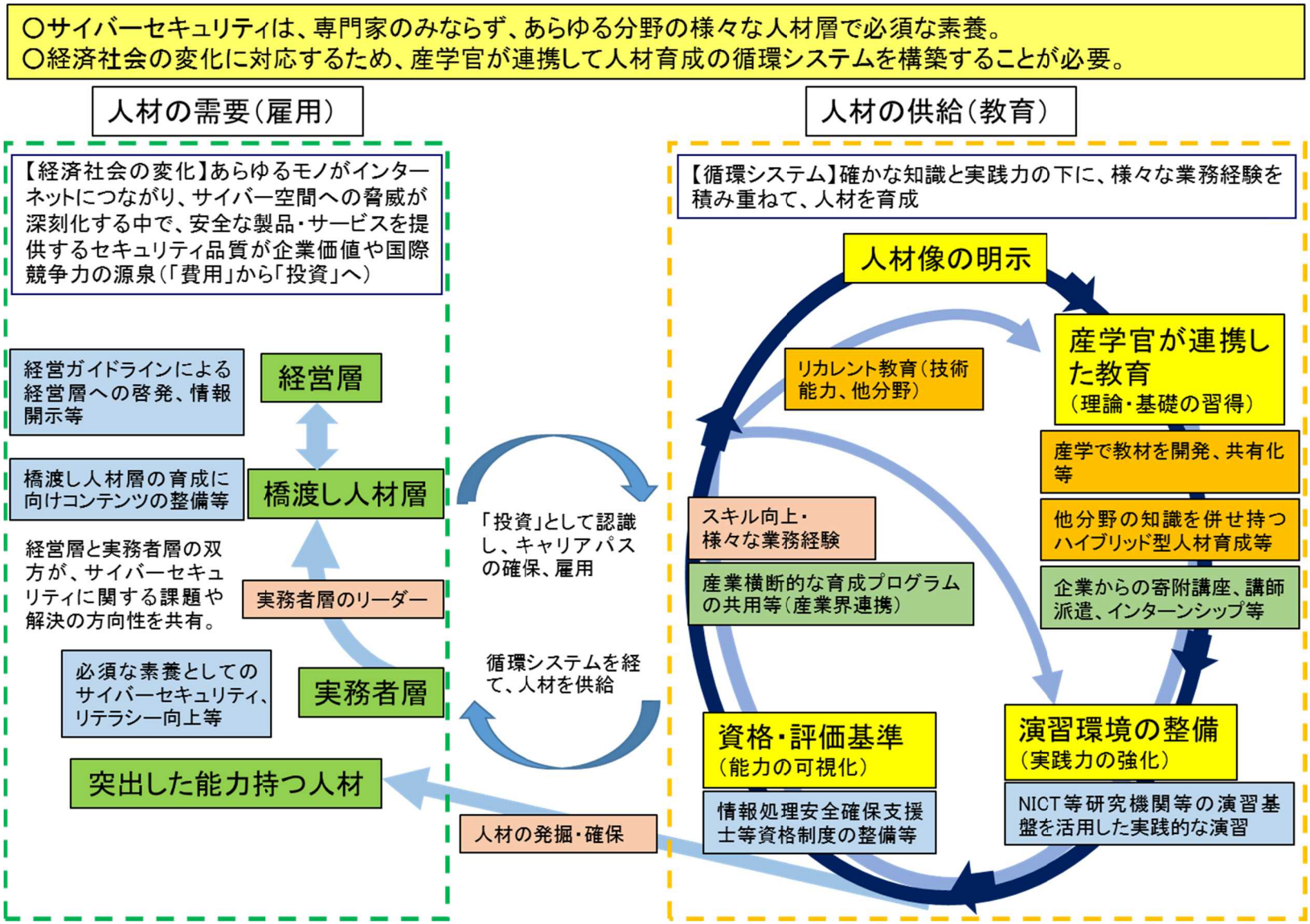

図2：社会で活躍できる人材の育成

Ⅱ　今後の検討の枠組み

・それぞれの取組・施策をつなげる「つなぐ取組」について、平成 28 年6月を目途に方向性を定め、平成 28 年中を目途に具体的施策を提示する。
・「産学官の情報共有の場」として情報セキュリティ社会推進協議会産学官人材育成 WG で情報共有する。（継続・拡充）
・次期人材育成プログラムを策定・公表する。（平成 28 年度中）

本方針では、戦略で掲げた各取組を加速するため、企業等での取組、大学等での取組、政府が取り組む施策等を整理した。

「安全なサイバー空間」を実現するために、人材を育成し、雇用やキャリアパスを確保していくことが急務の課題であり、このためには、人材の需要と人材の供給の好循環を形成していくことが重要である。

特に、図2で示す民間部門における人材育成の循環システムを形成するためには、それぞれの取組・施策をつなげる取組（「つなぐ取組」）が必要であり、この「つなぐ取組」について、関係者での議論を深め、平成 28 年6月を目途に方向性を定め、平成 28 年中を目途に具体的な施策の提示を行う。

また、人材の需要と供給の好循環の構築に向けた「産学官の情報共有の場」として、「情報セキュリティ社会推進協議会産学官人材育成 WG」[15][16]において情報共有を図る。そこでの検討を踏まえ、政府として取り組む施策については、本方針に基づく各施策の進捗状況及び評価を行いつつ、普及啓発・人材育成専門調査会において審議し、次期人材育成プログラム（3年程度を視野）に盛り込むこととし、平成 28 年度中に策定・公表する。

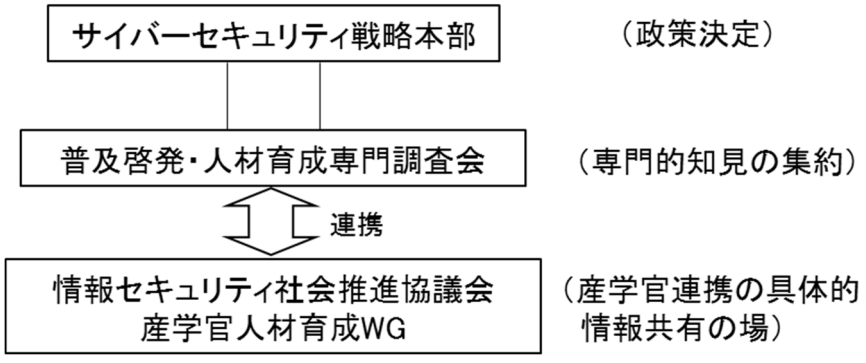

図3：サイバーセキュリティ人材育成に係る今後の検討の枠組み

15 「情報セキュリティ社会推進協議会」は国民全体の情報セキュリティ及び安全・安心なICT利活用に対する意識向上に向け、国及び地域の産学官民が普及啓発活動に関する情報流通網を構築し、各主体の連携・協力を通じて、安全・安心な社会を構築することを目指すため設立された協議会。

16 「産学官人材育成 WG」は人材の需要（雇用）と供給（教育）の好循環の構築に向け、産学官が情報を共有し、地域の枠を超えて連携・協力して人材育成を進めていくための議論を行う場として、情報セキュリティ社会推進協議会の下に設けられた産学官の関係者からなるワーキンググループ。