参考資料

サイバーセキュリティ人材育成総合強化方針

平成 28 年3月 31 日
サイバーセキュリティ戦略本部

目　次

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、第1章において、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。次に、第2章では、政府機関における専門人材育成、一般職員のリテラシー向上等についての取組方針を示す。そして、第3章において、今後の検討の枠組みを示す。

第1章　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よう人材の裾野を拡大し、その能力の底上げを図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。

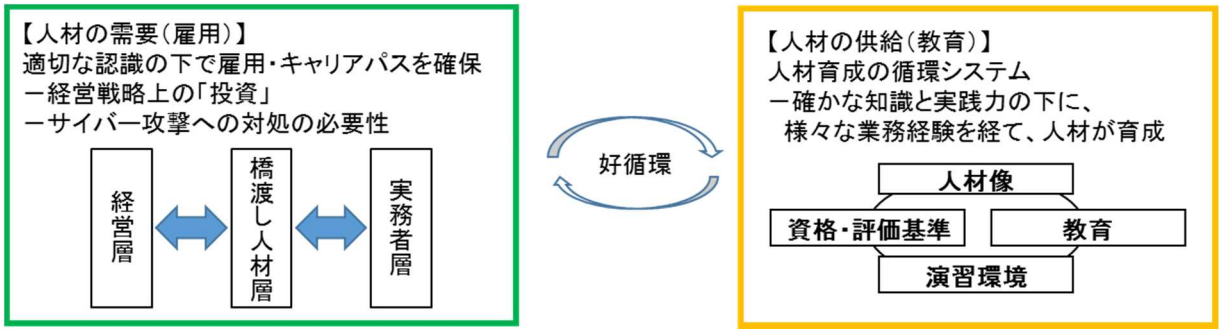

図1：サイバーセキュリティ人材育成に係る需要と供給の好循環（概念図）

1　情報通信技術（Information Technology）の略称

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る。このため、「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、サイバー空間における悪意ある活動は、あらゆるモノ・サービスに影響を及ぼし、その損害が飛躍的に大きくなる。そのような中で、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、危機意識を持ってリスクマネジメントに当たることが必要である。また、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多様な関係者(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利用者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に基づくサイバーセキュリティ対策を実践し、実務課題を踏まえた経営戦略を提示し、さらに、組織内の関係部局間の総合調整や実務者層をまとめリードすることができる橋渡し人材層が必要であり、その育成を推進する。

また、橋渡し人材層には、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[5]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、いったん就職した後に、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当たっては、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。

なお、サイバーセキュリティに係る人材においては、技術的な能力のみならず、高い倫理観も同時に身に付ける必要がある。

（1）求められる人材像の明示

・人材育成施策において目標とす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。

サイバーセキュリティの素養については、IT製品・サービスのベンダー企業でITを扱う技術者のみならず、製品の生産やサービスの提供を行っている者、その利用者に至るまで、様々な層の人材に必須のものとなりつつある。また、IT製品・サービスのベンダー側の立場のみならず、ユー

5 リカレント教育：職業人を中心とした社会人に対して、学校教育の修了後、いったん社会に出てから行われる教育であり、職場から離れて行われるフルタイムの再教育のみならず、職業に就きながら行われるパートタイムの教育も含む。

ザー側の立場の双方において、「橋渡し人材層」、「実務者層」ごとに求められる人材像は異なってくると考えられる[6]。

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」（複合型人材）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必要規模も含めた人材像の明確化等を目標として検討する動きがあり[7]、そうした人材の需要側の動向に応えるためにも、人材育成施策において目標とする人材像の明確化について検討を進め、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当たり、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

6 「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
7 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。

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、

- 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[8]）」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文部科学省が認定する「職業実践力育成プログラム（BP[9]）」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[10]」制度等により、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

8 Education Network for Practical Information Technologies の略称（「エンピット」と読む）。複数の大学と産業界による全国的なネットワークを形成し、実際の課題に基づく課題解決型学習等の実践的な教育を推進することにより、情報技術を活用して社会の具体的な課題を解決できる人材の育成を強化することを目的とした事業。平成 24 年度から実施。

9 Brush up Program for professional の略称。大学・大学院・短期大学・高等専門学校におけるプログラムの受講を通じた社会人の職業に必要な能力の向上を図る機会の拡大を目的として、平成 27 年7月に認定制度を創設。同年 12 月に 123 課程を初回認定した。

10 専修学校の専門課程であって、職業に必要な実践的かつ専門的な能力を育成することを目的として専攻分野における実務に関する知識、技術及び技能について組織的な教育を行うものを、「職業実践専門課程」として文部科学大臣が認定する制度。平成 26 年4月から認定された学科がスタート。

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[11]）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[12]のLAN[13]管理者のサイバー攻撃への対応能力向上のため、実践的なサイバー防御演習（CYDER[14]）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、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）

11 National Institute of Information and Communications Technology の略称
12 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。
13 Local Area Network の略称
14 CYber Defense Exercise with Recurrence の略称。職員が数千人規模の組織内ネットワークを模擬した大規模環境を用いた実践的なサイバー防御演習。平成 25 年度より実施。

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。

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 年までに3万人超の有資格者の確保を目指す。これに向け、産学官が連携して、CYDER に加え国内外の企業等で行っている演習等の活用や大学における育成カリキュラムの導入支援等を推進する。

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 年度中に取りまとめる。

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当たっては、利用者である産業界や大学等社会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）[15]が整備するITスキル標準[16]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）

また、サイバーセキュリティに関する業務に従事する者に対しては、例えば自組織内のシステムでトラブルが発生したことにつき負の評価がされるというのでなく、トラブルを未然に防止したことについて正当な評価がなされることが必要である。このため、能力を可視化した上で、産業界

15 Information-technology Promotion Agency の略称
16 各種IT関連サービスの提供に必要とされる能力を明確化・体系化した指標であり、産学における教育・訓練等に有用な「ものさし」（共通枠組）を提供しようとするもの。平成 14 年に経済産業省が策定・公表。

やセキュリティ関連業務を行う独立行政法人を含め政府関係機関等において業務に従事する者にその能力や実績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[17]」や「未踏IT人材発掘・育成事業[18]」のような挑戦の機会を設け、参加を促すことによって、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、海外から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。

17 若年層のセキュリティ人材を発掘・育成するため、22 歳以下の学生を対象とした、産業界、教育界を結集した講師による講習・演習を行う合宿事業。平成 16 年よりIPAが実施し、現在は民間企業と連携し実施。
18 ITを駆使してイノベーションを創出することのできる独創的なアイディアと技術を有するとともに、これらを活用する優れた能力を持つ、突出した若い人材を発掘・育成することを目的とした事業であり、平成 12 年度からIPAが実施。

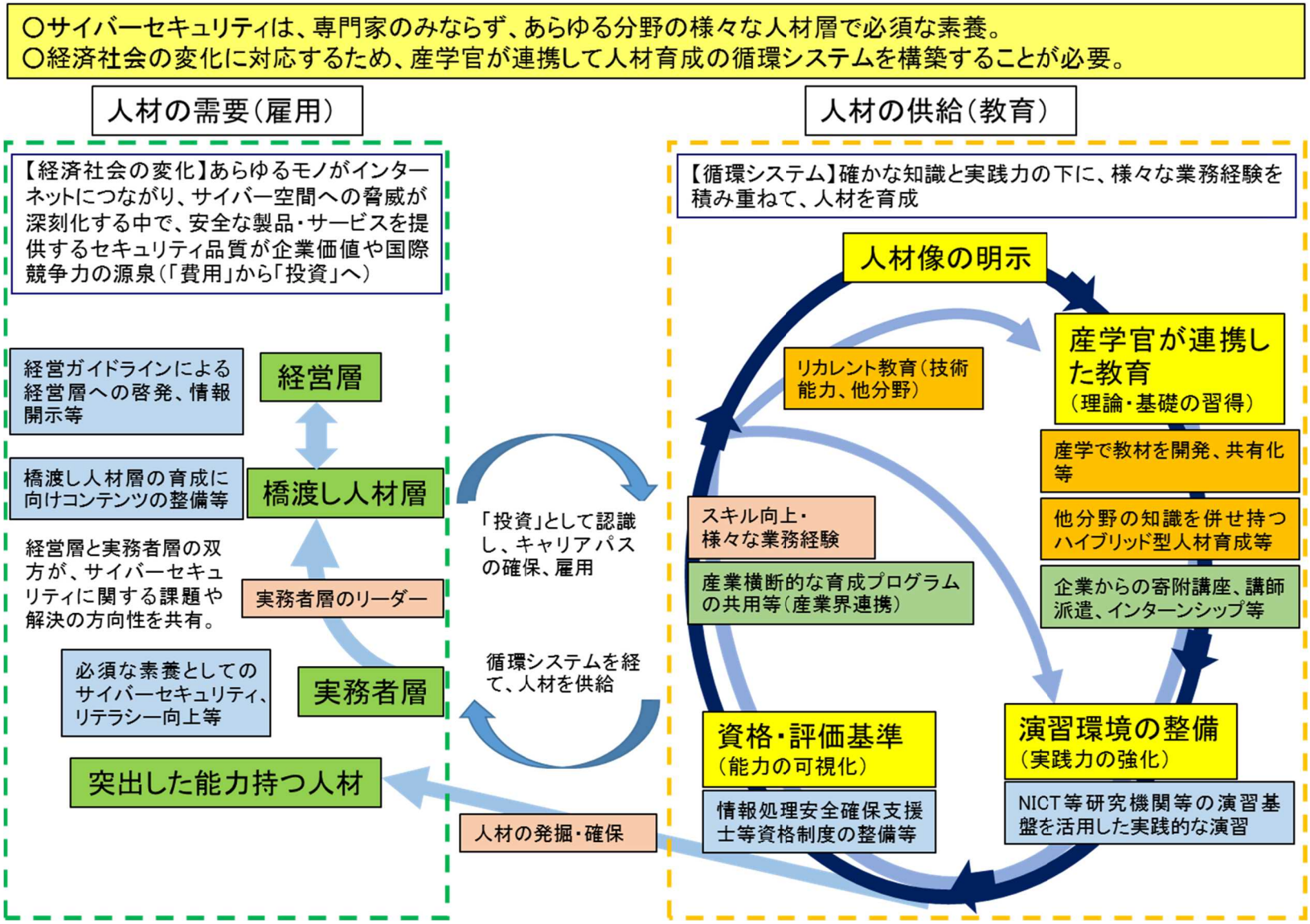

図2：社会で活躍できる人材の育成（イメージ）

第2章　政府機関におけるセキュリティ・IT人材の育成

政府機関においても、近年のサイバーセキュリティ事案の増加等に鑑み、情報システムの適切な運用管理とサイバーセキュリティ対策及びこれらと一体となった業務改革等に取り組み、セキュリティを確保しつつ効率的な行政運営の実現を図ることが必要である。

一方、政府機関における課題として、セキュリティに係る人材が圧倒的に不足しているとともに、システム管理や業務改革に関する知識・経験を有する人材も不足していること、加えて、一般職員の情報リテラシーも不十分であること、また、自組織におけるセキュリティ対策等の司令塔機能も弱体であること等が挙げられる。このため、これらの課題解決に向け、①司令塔機能の抜本的強化、②高度専門人材と一般行政部門との橋渡しとなるセキュリティ・IT人材（橋渡し人材）の確保・育成、③即戦力人材としての民間の高度専門人材の確保、④一般職員の情報リテラシー向上の実現を図ることが必要である。

各府省庁におけるセキュリティ・ITに係る体制・人材に関しては、近年急速な進展が見られ、かつ、今後も目まぐるしく変化が生ずることが想定される分野であるため、各府省庁の所管業務ではあるものの、こうした進展や変化に応じた適切な対応が困難な面があること、また、インシデント対応、システム管理など、業務としての共通点が認められることに加え、育成すべき人材なども共通している面が大きいため、各府省庁それぞれで対応するのではなく、政府全体で目指すべき方向性を共有し、横断的な連携を図りながら、方策を進めていくことが効果的であると考えられることから、政府機関において取り組むべき方針として以下を示す。なお、方針に基づく取組は適宜見直していくものとする。

1．各府省庁における司令塔機能の抜本的強化

各府省庁においては、平成 28 年度から、サイバーセキュリティ・情報化審議官の新設等により、情報システムの適切な運用管理とサイバーセキュリティ対策及びこれらと一体となった業務改革等について、最高情報セキュリティ責任者（CISO）と情報化統括責任者（CIO[19]）を補佐し、府省庁内を指揮監督できる強力な体制を構築する。

また、サイバーセキュリティ・情報化審議官等の主導の下、組織規模や所管するシステム等の実情を踏まえつつ、人材の着実な確保・育成を図るため、速やかに、採用、人材育成、将来像等にわたる具体的な取組方策を定めた「セキュリティ・IT人材確保・育成計画（仮称）」を作成し、各府省庁のサイバーセキュリティ・情報化審議官等で構成する会議において共有の上、フォローアップを実施する。当該計画の下で、有為な人材を確保するとともに、「セキュリティ・IT人材育成支援プログラム（仮称）」を設け、当該プログラムを通じ、セキュリティ・ITに係る業務に充てるべき人材を育成する。

19 Chief Information Officer の略称

内閣官房等においては、当該計画及びプログラムの作成、当該人材の確保・育成を支援する。

各府省庁の取組状況については、サイバーセキュリティ対策推進会議（CISO等連絡会議）、各府省情報化統括責任者（CIO）連絡会議や次官連絡会議においても共有を図る。

2. 橋渡し人材（部内育成の専門人材）の確保・育成

セキュリティに関して対応が求められる事案の急増、システムによる更なる業務効率化の推進など、セキュリティ・ITに係る業務の増加、複雑困難化がみられる中で、各府省庁における現在のセキュリティ・ITに係る体制は脆弱（ぜいじゃく）であり、各府省庁を中心に橋渡し人材を確保・育成することが喫緊の課題であることから、体制や人材に係る実態を把握した上で、「セキュリティ・IT人材（橋渡し人材）」として、「セキュリティ・ITに関する一定の専門性と、所管行政に関する十分な知識・経験を有し、高度専門人材[20]と一般行政部門との橋渡しをする人材」を相当数確保・育成する必要がある。ついては、以下のとおり、(1)体制の整備・人材の拡充、(2)有為な人材の確保、(3)一定の専門性を有する人材の育成、(4)研修体系の抜本的整理、(5)適切な処遇の確保に係る取組を実施することとする。

（1）体制の整備・人材の拡充

・各府省庁の統括部局の体制の整備及び人材の拡充を行う。（平成 28 年度から順次実施）
・併せて、各府省庁の一定のシステム所管部局の体制の整備及び人材の拡充を行う。（統括部局の体制整備等も踏まえつつ段階的に実施）

各府省庁のセキュリティ・ITに係る統括部局の体制の整備及び人材の拡充を実施する。また、当該整備及び拡充と併せて、各府省庁の社会的な影響の大きいシステムを所管する部局についても体制の整備及び人材の拡充を実施する。

（2）有為な人材の確保

・政府一体となって、各府省庁参加の合同説明会、内閣人事局による各種広報等における積極的な広報を実施する。（可能なものは平成 28 年度から実施）
・将来的に、大学等での「出張講義」、職場での業務体験イベントやインターンシップの実施などを検討する。（可能なものは平成 29 年度から実施）
・各府省庁において有為な人材を確保する。（平成 29 年度から順次実施）

政府機関におけるセキュリティ・IT人材の確保・育成に向けた取組に対する学生等の関心を高

20 セキュリティ・ITに関する高度な専門性を有する民間等の人材

めることで、当該人材の志望者の拡大を図るため、府省庁横断的な人材のニーズを踏まえ、政府一体となって、各府省庁参加の合同説明会、内閣人事局による各種広報等の中央の採用活動における積極的な広報を実施する。

将来的に、産学官が連携した教育の充実に併せて、情報系の大学・学部等を対象にした「出張講義」の実施、学生等を対象とした職場での業務体験イベント（事案対応シミュレーション等）やインターンシップの実施などのほか、有為な人材の確保に向けた更なる方策を検討する。

各府省庁において、セキュリティ・ITに係る素養の把握に努め、セキュリティ・IT人材に求められる資質を十分に考慮し、適性が認められる者を採用（新卒採用のほか、実務経験者の選考による中途採用も可能）するなどにより、有為な人材を確保する。

（3）一定の専門性を有する人材の育成

・各府省庁において、「セキュリティ・IT人材育成支援プログラム（仮称）」を設け、一定の専門性を有する人材を育成する。（平成 29 年度から順次実施）
・将来的に、一部の人材を総務省行政管理局等で採用・一括管理し、各府省庁等に派遣する枠組みを検討する。（各府省庁の人材育成に目途が立った段階での実施に向け検討）

各府省庁において、適切な人材育成を図るための「セキュリティ・IT人材育成支援プログラム（仮称）」を設け、橋渡し人材にとっても魅力あるものとなるよう、当該プログラムの中で、各府省庁における一般行政事務従事等により、所掌事務に関する十分な知識・経験を習得させつつ、セキュリティ・ITに係るスキルレベルの確保や能力向上を図るため、各府省庁のシステムのライフサイクル経験とともに、セキュリティについては、事案対処、保安、事故対応、危機管理、安全保障等の業務に従事させるほか、橋渡し人材に共通した取組として、役職段階ごとの研修受講（原則必須化）、内閣官房内閣サイバーセキュリティセンター（NISC[21]）・内閣官房情報通信技術（IT）総合戦略室（IT室）・総務省行政管理局・個人情報保護委員会への出向（原則必須化）、国内外の大学院・民間企業への派遣、NICTが整備する人材育成施設の活用などを通じ、一定の専門性を有する人材を育成する。

また、将来的に、一部の人材を総務省行政管理局等で採用して一括で管理し、各府省庁等への派遣を可能とする枠組みについても検討を行う。

21 National center of Incident readiness and Strategy for Cybersecurity の略称

（4）研修体系の抜本的整理

・現行の研修体系の抜本的整理、研修修了者にスキル認定を行う枠組みの構築等を行う。（可能なものは平成 28 年度から実施）
・管理職に実践的な演習等に係る研修を実施する。（可能なものは平成 28 年度から実施）
・CSIRT要員への研修・訓練を活用する。（平成 28 年度から実施）

NISC及び総務省行政管理局等において、橋渡し人材のセキュリティ・ITに係る能力の向上を図るため、橋渡し人材としての研修受講者数を今後 4 年間で 1000 人を超える規模とすることを目指して、役職段階別（係員、係長など）のスキルレベルのモデルを設定し、これに応じた現行の研修体系の抜本的整理を行うとともに、研修修了者にスキル認定を行う枠組みを構築するほか、研修の受講履歴を体系的に整理して各府省庁の人事担当者と情報共有を行う枠組みを検討する。

また、管理職向けに、NISC及び総務省行政管理局等において、基本的なセキュリティ・ITについての素養を身につけるための研修、業務・システム改革やサイバーセキュリティのケーススタディなどの実践的な演習等に係る研修を実施する。

また、CSIRT[22]要員への研修や訓練についても活用していく。

（5）適切な処遇の確保

・業務の専門性・特殊性等を踏まえ、手当等を新たに支給することによる一定の給与上の評価を行う。（平成 29 年度から順次実施）
・「セキュリティ・IT人材確保・育成計画（仮称）」の中で、出向等の機会を捉えた昇任等も含め、高位のポストまでを見据えた人事ルート例（イメージ）を設定する。（平成 28 年度に速やかに実施）

セキュリティ・ITに係る業務の専門性・特殊性等とともに、適切な育成がなされた人材が充てられることを踏まえ、手当等を新たに支給することによる一定の給与上の評価を行う。

各府省庁のセキュリティ・IT人材は、「セキュリティ・IT人材育成支援プログラム（仮称）」を通じて、所掌事務に関する十分な知識・経験を得つつ、セキュリティ・ITに係る能力も向上させることにより、的確な育成が図られる人材であることから、有為な人材には、適切な時期にセキュリティ・ITに係る枢要なポストへ昇任させるなど、これに相応しい処遇が確保されることが必要である。そのため、各府省庁において、「セキュリティ・IT人材確保・育成計画（仮称）」の中で、出向等の機

22 府省庁において発生した情報セキュリティインシデントに対処するため、当該府省庁に設置された体制をいう。
Computer Security Incident Response Team の略称

会を捉えた昇任等も含め、高位のポストまでを見据えた人事ルート例（イメージ）を設定する。

３．外部人材（即戦力の高度専門人材）の確保

セキュリティ人材については、NISC等において、平成 28 年度から民間の特に高度なセキュリティ人材を特定任期付職員等の制度を活用して採用し、必要に応じて監査等を通じ各府省庁に派遣する。

IT人材については、IT室において、一元的に採用・管理（プール制）している政府CIO補佐官を積極的に活用し、引き続き必要な人材を各府省庁に派遣する。

また、政府において必要な即戦力となる外部人材を確保していくため、我が国に実践的な能力を有するセキュリティ人材の層の充実を積極的に図るための施策を推進する。具体的には、enPiTの枠組みを活用した産学のネットワークの構築、産学官が連携した教育の充実、NICT等の演習基盤を活用した実践的演習の強化、「情報処理安全確保支援士」等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等の整備等を推進する。

４．一般職員の情報リテラシー向上

各府省庁の新人研修等において、セキュリティ・ITに関する各種研修を実施する。なお、当該研修に利用可能な研修教材として、NISCや総務省行政管理局から各府省庁にコンテンツを提供する。その際、e-learning 等による実施や、そのためのセキュリティ・IT教材の共通化なども併せて検討する。さらに、採用予定者に対して研修教材を提供することについても併せて検討する。これらについて、可能なものは平成 29 年度から実施していく。

内閣人事局が行う新任の管理職を対象とした研修において、管理職に必要な基礎的能力の向上の一環として、セキュリティ・ITに関する基礎的知識を得る機会を引き続き提供する。

内閣人事局が作成する「人事評価マニュアル」を改訂し、セキュリティ、危機管理、IT利活用等について取られた行動に関する評価の着眼点を明示する。また、内閣人事局が実施する評価者訓練においても周知する。これらについて、可能なものは平成 28 年度から実施していく。

〔参考1〕

政府機関におけるセキュリティ・IT人材育成総合強化方針（案）【概要】

【政府機関におけるセキュリティ・IT人材の育成】
1. 各府省庁における司令塔機能の抜本的強化
2. 橋渡し人材（部内育成の専門人材）の確保・育成
3. 外部人材（即戦力の高度専門人材）の確保
4. 一般職員の情報リテラシー向上

1. 各府省庁における司令塔機能の抜本的強化

各府省庁CISO／CIO

直接補佐

サイバーセキュリティ・情報化審議官等

情報システムの適切な運用管理とサイバーセキュリティ対策及びこれらと一体となった業務改革等について専任で指揮監督

主導

セキュリティ・IT人材確保・育成計画（仮称）

指揮監督

民間等におけるセキュリティ・IT高度専門人材（①）

橋渡し人材
セキュリティ・ITの一定の専門性と所管行政の知識・経験を有し、①と②との橋渡しをする人材

一般行政部門（②）

2. 橋渡し人材（部内育成の専門人材）の確保・育成

(1)体制の整備・人材の拡充
- 各府省庁の統括部局・一定のシステム所管部局の体制の整備・人材の拡充

(2)有為な人材の確保
- 積極的な広報のほか、大学等での出張講義、インターンシップなどを検討
- 各府省庁において有為な人材を確保

(3)一定の専門性を有する人材の育成
- 「セキュリティ・IT人材育成支援プログラム（仮称）」の作成（研修受講、NISC等への出向、大学院・民間企業への派遣等を通じた人材育成）
- 総務省行政管理局等で一部人材の採用・一括管理の枠組み検討

(4)研修体系の抜本的整理
- 新たに役職段階別に研修体系を抜本的整理（橋渡し人材の受講者数を今後4年で1千人超規模を目指す）、修了者にスキル認定を行う枠組みの構築等
- 管理職に実践的な演習等に係る研修を実施
- CSIRT要員への研修・訓練の活用

(5)適切な処遇の確保
- 業務の専門性・特殊性等を踏まえ、手当等を新たに支給することによる一定の給与上の評価
- 高位のポストまでを見据えた人事ルート例（イメージ）の設定

3. 外部人材（即戦力の高度専門人材）の確保

産学のネットワーク構築、産学官連携での教育の充実、NICT等の演習基盤の活用、情報処理安全確保支援士等の整備等の推進

NISC等での高度なセキュリティ人材の採用と監査等を通じた各府省庁への派遣、IT室において政府CIO補佐官の積極的活用

4. 一般職員の情報リテラシー向上

- 各府省庁の新人研修等でのセキュリティ・IT研修実施
- 新任管理職研修でのセキュリティ・ITの基礎的知識の習得機会提供
- 人事評価マニュアル改訂（セキュリティ等に係る行動の評価の着眼点を明示）等

橋渡し人材の育成に向けた研修体系の抜本的整理

〔参考2〕

従来のプロジェクト管理、システム運用・保守等主としてテーマ別となっている研修体系から、橋渡し人材の各役職に必要なスキル全般を段階的に得られるよう、新たな役職段階別の研修体系に向け、順次、抜本的に整理。新たな研修体系では、受講を原則必須化。

役職	役職段階別の研修
管理職	○ 基本的なセキュリティ対策・ITについての素養の強化、業務・システム改革やサイバーセキュリティのケーススタディなどの実践的な演習等に係る研修を実施
課長補佐	
係長	○ 係長時に担当業務に応じて適宜受講し、課長補佐昇任までに一通り修了すべき研修コース
係員	○ 係長昇任までに一通り修了すべき研修コース ○ 採用後速やかに受講・修了すべき研修コース

※ 上記のほか、OJTとしてNISC・IT室・総務省行政管理局・個人情報保護委員会への出向、国内外の大学院・民間企業への派遣などを通じて人材を育成。

第3章　今後の検討の枠組み

【社会で活躍できる人材の育成】

・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」[23][24]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の確認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。

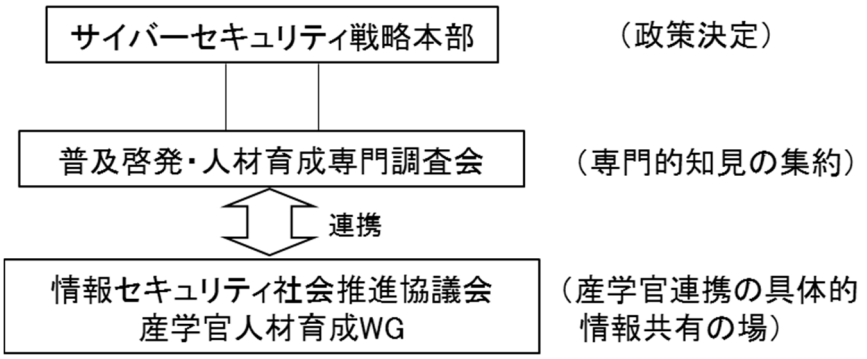

図3：社会で活躍できるサイバーセキュリティ人材育成に係る今後の検討の枠組み

23 「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。

24 「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。

【政府機関におけるセキュリティ・IT人材の育成】

・平成 28 年度よりサイバーセキュリティ対策推進専任審議官等会議及び各府省情報化専任審議官等連絡会議を設置する。
・各府省庁において「セキュリティ・IT人材確保・育成計画（仮称）」を作成する。同計画において「セキュリティ・IT人材育成支援プログラム（仮称）」を設ける。

政府機関におけるセキュリティ・IT人材の育成については、平成 28 年度より政府一体となって各種取組を進めるため、サイバーセキュリティ・情報化審議官等で構成する会議（サイバーセキュリティ対策推進専任審議官等会議及び各府省情報化専任審議官等連絡会議）を設けるとともに、各府省庁においては、同審議官等の主導の下、採用、人材育成、将来像等にわたる具体的な取組方策を定めた「セキュリティ・IT人材確保・育成計画（仮称）」を作成する。また、当該計画において、研修受講、NISC等への出向、大学院・民間企業への派遣等に係る「セキュリティ・IT人材育成支援プログラム（仮称）」を設け、同プログラムを通じてセキュリティ・IT人材の育成を図る。

なお、これらの取組状況は、CISO等連絡会議、CIO連絡会議及び次官連絡会議において共有を図るとともに、取組は適宜見直していくものとする。

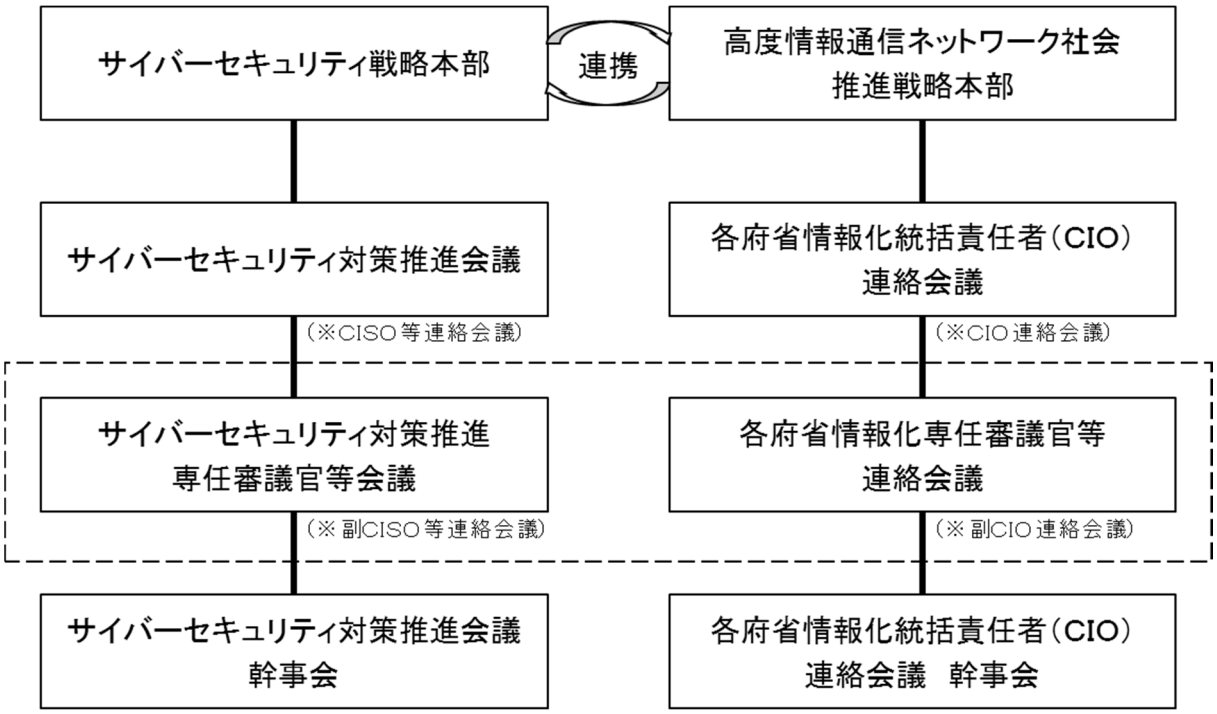

図4：政府機関におけるセキュリティ・IT人材育成に係る今後の検討の枠組み