資料２

サイバーセキュリティ人材育成プログラム（案）

資料２－１　「サイバーセキュリティ人材育成プログラム（案）」の全体概要

資料２－２　サイバーセキュリティ人材育成プログラム（案）

資料２－３　「サイバーセキュリティ人材育成プログラム（案）」に対する意見募集の結果の概要

資料２－４　意見募集に対して寄せられたご意見の概要及びご意見に対する考え方

「サイバーセキュリティ人材育成プログラム（案）」の全体概要

資料2－1

現状と課題

〇脅威は更に深刻化、これまでの人材育成の取組は一定の成果を得つつも専門性を高める取組等一層の充実が必要。

〇 ITの利活用により、新しい価値を創造するビジネスイノベーションと一体となったサイバーセキュリティへの取組が必要。

→ビジネスにおけるそれぞれの役割の中で、サイバーセキュリティ全体を俯瞰でき、関連するサイバーセキュリティを実践できる人材の育成が必要。

〇ビジネスイノベーションを生み出せるサイバーセキュリティ人材の育成が必要。また、将来的な社会変化に対応するため、セキュリティに対する意識を若年層から高めることが必要。

今後の取組方針

【基本方針】　需要（雇用）と供給（教育）の好循環の形成

〇これまでの取組に加え、ITの利活用により新たな価値を創造するためのサイバーセキュリティ人材育成が必要。

・経営層：サイバーセキュリティを実務者層だけの問題ではなく経営問題として捉えるとともに、新たな価値の創造という「挑戦」に付随する「責任」としてサイバーセキュリティに取り組むという意識改革を図る。

・橋渡し人材層：経営層・実務者層のコーディネーターにとどまらず、ビジネス戦略と一体となってサイバーセキュリティの企画・立案を行い、実務者層を指揮できる橋渡し人材層の育成に取り組む。

・実務者層：情報セキュリティ技術に関する知識・能力の向上だけでなく、チームとなってサイバーセキュリティを推進するための人材育成に取り組む。

・高度人材（高等教育段階を含む）：高度なセキュリティ技術の専門性を持ちつつ、ビジネスイノベーションを創出する高度人材の育成に取り組む。

・初等中等教育段階：児童生徒の情報活用能力（プログラミング的思考や情報セキュリティ、情報モラルを含む）を培う。

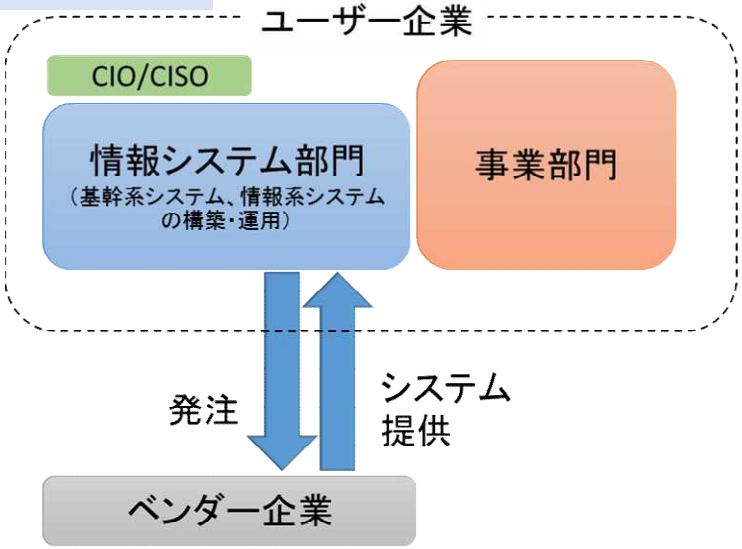
〇これまでの取組と新たな取組の質的向上を図るため、施策間連携の場をつくり、具体化（例：モデルとなるカリキュラムの策定）を図る。

まとめ

産学官の取組状況や施策間連携の検討状況、サイバーセキュリティ人材を取り巻く課題について、フォローアップを行い、必要に応じて本プログラムの見直しを検討。

ITの利活用に関する変化への対応（体制例）

業務の効率化

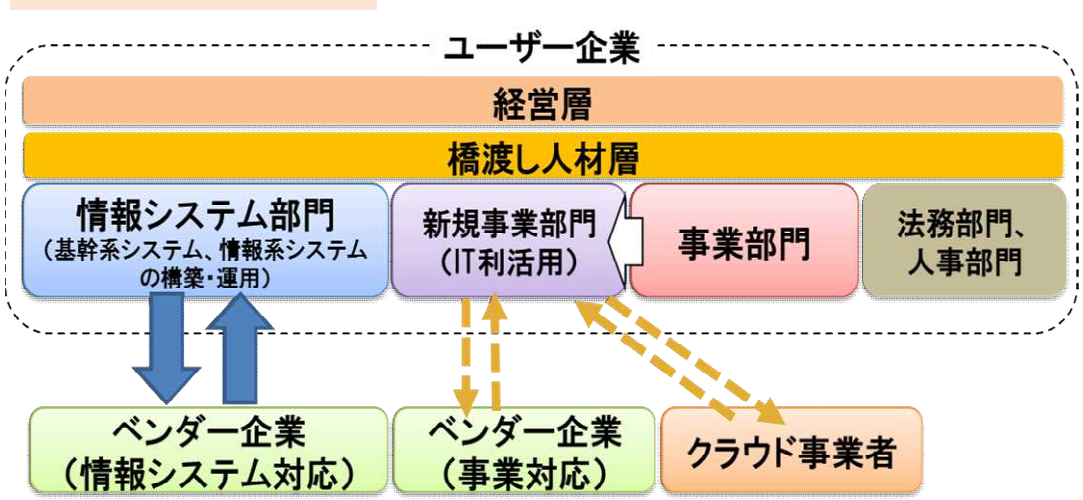


ITの利活用による業務効率化等を目的として、情報システム部門がベンダー企業から基幹系システム（生産・販売、会計、人事、給与、資産の管理等に関する企業内のシステム）や情報系システム（メールや文書作成、スケジュール管理等に関するシステム）を調達。

【特徴】

・ユーザー企業のニーズ（要件）は、明確であり、個々の事業に左右されにくい
・システム構築の時間軸は数年単位
・ベンダー企業は固定していることが多い

新たな価値の創造



IoTやビッグデータ、AIなど、ITの利活用により新しい価値を創造するような新規事業（ビジネスイノベーション）への挑戦においては、事業部門がベンダー企業やクラウド事業者などからシステムを調達。

【特徴】

・ユーザー企業のニーズ（要件）は、事業の試行錯誤と連動
・システム構築の時間軸は短く、事業そのものに対する理解とスピード感が不可欠
・クラウド事業者など新たなベンダーが関与することがある

注1：情報システム部門は社内向けの組織であり、新規事業部門は、社外向けの事業遂行組織を想定している。また、ここでは便宜上「新規事業部門」としているが、既存の「事業部門」内で、ITの利活用により新しいビジネスモデルによる事業を行う場合も含む。
注2：各部門については、実務者層を想定している。

CISO:最高情報セキュリティ責任者　Chief Information Security Officerの略称
CIO:情報化統括責任者　Chief Information Officerの略称

		これまでの取組	新たな取組
セキュリティへの意識		業務効率化のための情報システムのセキュリティ	IoT、ビッグデータ、AIなど、ITの利活用により新しい価値を創造するための「挑戦」に付随するセキュリティ
主な対象		ITベンダー、セキュリティベンダー、 ユーザー企業の情報システム部門	経営企画部門、情報システム部門、事業部門、製造部門、法務部門、監査部門など企業内の幅広い組織
重視される能力		サイバーセキュリティのスペシャリストとしての深い知識と実践力を持つこと	経営、IT、事業、製造、法務などそれぞれの役割を担うエキスパートとして関連するサイバーセキュリティの知識を持ち、異なるエキスパートやスペシャリストとチームとなって業務ができること
人材の規模		現在の人材：26.5万人（不足数：8.2万人） ※対企業アンケート（情報セキュリティ人材）をベースに不足数を推計（2014年のIPA推計）	現在の人材：28.1万人（不足数：13.2万人）＋認識されていない人材 ※対企業アンケート（事業部門も対象）をベースに不足数を推計（2016年の経済産業省推計）
取組（需要）	経営層	経営層が経営戦略の一環として情報セキュリティ対策を捉えることが重要（実務者任せにしない）。地域を含めた中小企業の人材育成を推進。 ・「サイバーセキュリティ経営ガイドライン」の策定や中小企業向けの普及啓発	「挑戦」とそれに付随する「責任」として、リスクの一項目としてのサイバーセキュリティに取り組むことが重要。 ・「企業経営のためのサイバーセキュリティの考え方」を踏まえたフォローアップ、普及啓発
（供給）	橋渡し人材層	実務者層のリーダー層が経営層との調整を含めたコーディネーター（橋渡し役）となることが重要	ビジネス戦略と一体となってサイバーセキュリティの企画・立案し、経営層に説明し、実務者層（技術者等）を指揮する人材が重要 ・橋渡し人材層向けのセミナー等の開催、情報処理安全確保支援士の活用、学び直しプログラムの活用
	実務者層	情報セキュリティ技術に関する知識・能力を高めることが重要 ・職業実践力育成プログラムを通じたセキュリティ技術人材の育成（例：東京電機大学CySec）、実践的サイバー防御演習（CYDER）、情報処理安全確保支援士の創設	チームとなって推進するための人材育成の取組が重要 ・社会人の学び直しプログラムの活用（enPiT、産業サイバーセキュリティセンター）、高等専門学校における情報系学科の学生にとどまらないセキュリティ教育、セキュリティマネジメント試験の活用
	高度人材（高等教育を含む）	高度なサイバーセキュリティ技術の専門性を持つ人材育成が重要 ・大学学部生・院生の育成（enPiT）、高専や専修学校における教育、若年層の人材発掘（セキュリティキャンプ）、サイバーコロッセオ	ビジネスイノベーションが実現できる高度なサイバーセキュリティ人材の育成が重要 ・若手セキュリティエンジニアの育成（ナショナルサイバートレーニングセンター）

IPA：独立行政法人情報処理推進機構 Information-technology Promotion Agencyの略称
CySec：国際化サイバーセキュリティ学特別コース Tokyo Denki University Special Course on Global Cyber Security の略称
CYDER：実践的なサイバー防御演習　CYber Defense Exercise with Recurrenceの略称
enPiT：「成長分野を支える情報技術人材の育成拠点の形成」事業 Education Network for Practical Information Technologiesの略称（「エンピット」と読む）
NISC：内閣サイバーセキュリティセンター、National center of Incident readiness and Strategy for Cybersecurityの略称

これまでの各取組は、着実に進展し、一定の成果。橋渡し人材層の取組等一層の充実を図る必要

これまでの取組と新たな取組の質的向上を図るため、NISCが中心となって、ワーキンググループを設置し、以下の取組を推進する。

〇具体的な施策間連携の強化（検討内容の例）
- モデルとなるカリキュラムの策定
- 実践的演習における共同実施やカリキュラムの共有
- 教育や演習の参加による資格試験の一部免除

資料２－２

サイバーセキュリティ人材育成プログラム

（案）

平成 29 年　月　日

サイバーセキュリティ戦略本部

目次

1　はじめに

(1)本プログラム策定までの経緯

これまで、

- 新・情報セキュリティ人材育成プログラム（平成 26 年５月策定）（平成 26 年度～平成 28 年度までの３年間を対象とし、中長期的課題に対する視点も盛り込んだもの）
- サイバーセキュリティ戦略（平成 27 年９月策定）
- 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月策定）

を策定してきた。

これらの文書の策定を通じ、サイバーセキュリティ人材育成においては、「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必要であることが示された。

一方、IT の利活用は、単なる企業の業務効率化によるコスト削減のみならず、IoT、ビッグデータ、AI などの活用に代表されるように、ビジネスにおいて新たな価値を創造するような「挑戦」に不可欠なものとなりつつある。こうした中、内閣サイバーセキュリティセンター（NISC）は、「企業経営のためのサイバーセキュリティの考え方」（平成 28 年８月策定）を策定した。これを踏まえて、ビジネスにおける「挑戦」とそれに付随する「責任」としてのサイバーセキュリティを実現する観点も含め、企業におけるサイバーセキュリティ人材に係る課題とその在り方を検討し、「サイバーセキュリティ人材育成プログラム」を策定した。

(2)本プログラムの趣旨・位置づけ

サイバー空間は、企業活動のグローバル化やデジタル化が進む中において、主に民間主体の投資や英知の集約により急速な拡大を遂げてきており、経済社会の活動基盤となっている。こうした中、サイバー攻撃は、情報等の窃取、社会システムの機能不全により、国民生活、さらには国際社会が危機にさらされる原因となりうる。このため、個人や組織を問わず、あらゆる主体がサイバーセキュリティに対する認識を深め、各主体の協力的かつ自発的な取組を通じて、その脅威に対処できる安全な空間としていかなければならない。こうした中、本プログラムでは、企業をはじめとする社会で活躍できるサイバーセキュリティに関連する人材育成の方向性を示すことにより、安全な経済社会の活動基盤としてのサイバー空間の形成に向けた環境整備を図るものである。具体的には、産学官の連携により、サイバーセキュリティ人材の「需要」と「供給」の好循環を形成するため、サイバーセキュリティ人材を取り巻く課題を明らかにし、それに対する産学官の人材育成戦略の方向性を示したものである。さらに、将来を視野に入れて、ビジネスにおけるイノベーションを実現するために必要なサイバーセキュリティ人材の育成や、若年層に必要な教育の

在り方についても示している。対象については、企業をはじめとする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役割を持つサイバーセキュリティに係る人材育成を想定している。また、対象とする期間については、基本的に 2020 年東京オリンピック・パラリンピック競技大会開催前までの今後３年間（2017 年度から 2019 年度）を想定しているが、中長期的課題に対する視点も盛り込んでいる。

２　　現状と課題

（１）これまでの取組とサイバー空間の脅威の深刻化への対応

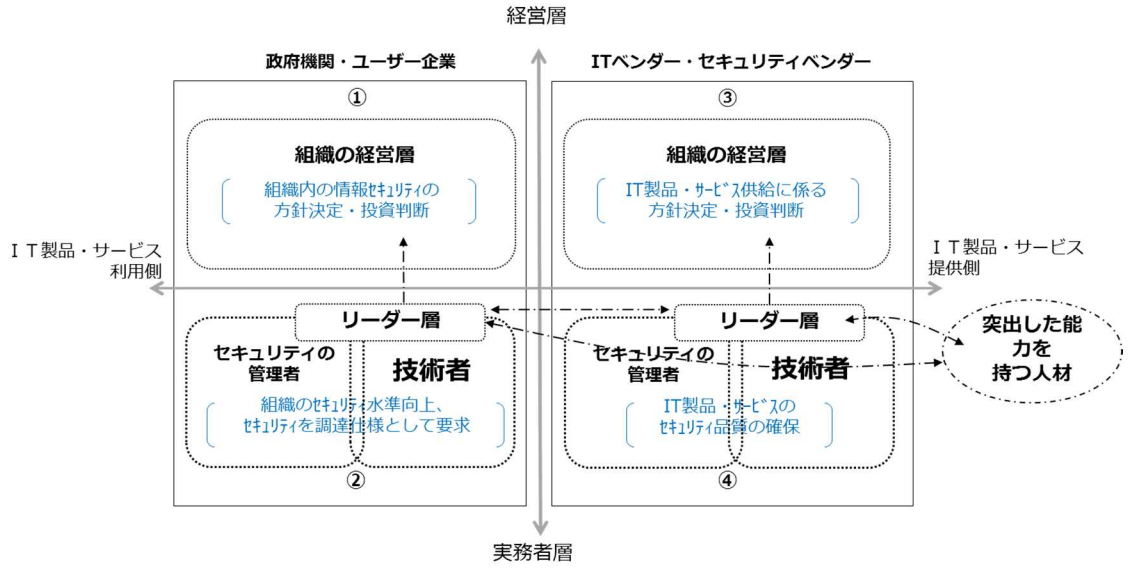
・　これまで、経営層の意識改革やユーザー企業・ベンダー企業のセキュリティの管理者・技術者といった実務者層の人材育成、突出した能力を持つ人材の発掘・育成の施策を推進し、一定の成果があった。サイバー空間における脅威の深刻化や人材の質・量の充実が課題であることを踏まえ、これまでの取組を引き続き推進していくことが重要である。

「新・情報セキュリティ人材育成プログラム」（平成 26 年５月策定）においては、図１に示すように、政府機関・ユーザー企業と、ベンダー企業（セキュリティベンダー企業を含む）のそれぞれについて、経営層の意識改革や実務者層（管理者や技術者）の育成、さらには、突出した能力を持つ人材の発掘・育成について必要な取組を示し、これまで関係省庁、関係機関が具体的な施策を実施してきた。経営層の意識改革については、実務者任せにすることなく、経営戦略の一環としてサイバーセキュリティ対策に取り組むため、「サイバーセキュリティ経営ガイドライン」を策定し普及活動を実施した。実務者層の育成については、サイバーセキュリティ技術に関する知識・能力を高めるための取組として、大学等における社会人向けのサイバーセキュリティに関する教育プログラムの充実や、実践的なサイバー防御演習などを実施した。また、情報処理安全確保支援士制度の整備を行った。さらに、高度な専門性を持った人材については、大学や高等専門学校における専門教育を実施したほか、セキュリティ技術と最新のノウハウを第一線の技術者から若手に伝授する「セキュリティ・キャンプ」の取組を通じ、突出した能力を持つ人材を発掘してきた。このように、「新・情報セキュリティ人材育成プログラム」に基づき、サイバーセキュリティ人材育成の取組については一定の成果があったといえる。

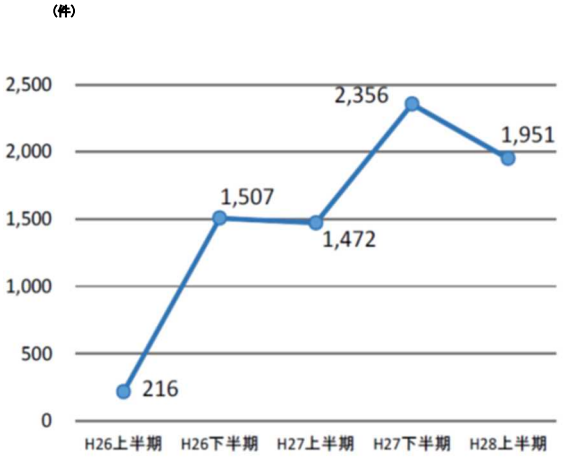
一方、サイバー空間上の脅威について、警察庁の調べによれば、標的型メール攻撃の件数は図２に示すように推移をしており、サイバー空間における探索行為についても図３に示すように、増加傾向にある。また、システムへのアクセスを制限し、その制限を解除するために身の代金を要求するいわゆるランサムウェア攻撃も深刻になっている。さらには、国家の関与が疑われるような組織的かつ極めて高度な攻撃も登場している。

こうしたサイバー空間における脅威の深刻化に対して、その利用環境が安全なものとなるよう、サイバー空間を構成する機器やサービスが安全かつ安定的に提供されることが不可欠である。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、その役割を担う政府機関・ユーザー企業と、IT ベンダー・セキュリティベンダー企業の実務者層（セキュリティの管理者や技術者）の育成や、突出した能力を持つ人材の発掘・育成に取り組み、人材の質・量を充実させていくことは引き続き重要な課題である。また、経営層については、引き続き意識改革が必要であるが、サイバーセキュリティ対策をやむを得ない「費用」とし

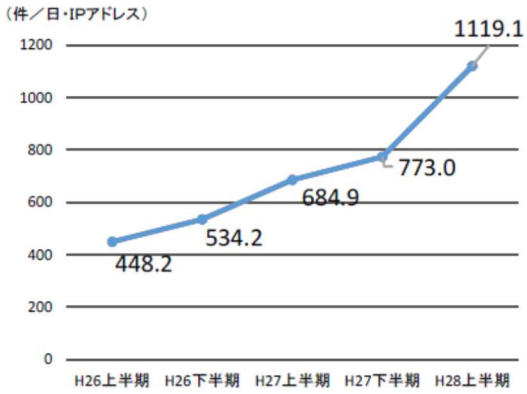
て認識するのではなく、IT の利活用の広がりに対応した新しい考え方が必要である。（詳細は後述することとする。）



（図１）「新・情報セキュリティ人材育成プログラム」で示された施策の対象分類



（図２）　標的型メール攻撃の件数の推移（※）



（図３）　警察庁がインターネットとの接続点に設置したセンサーに対するアクセス件数の推移

（※）平成 27 年下半期の標的型メール攻撃が突出しているのは同一内容のメールを複数の対象に送付する「ばらまき型」の攻撃が大きく増加したことが主な要因である。

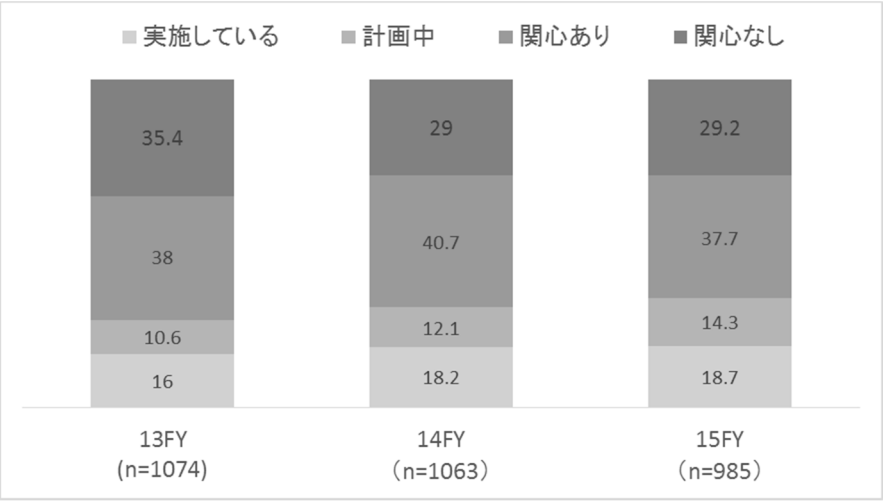
出典：警察庁　平成 28 年上半期におけるサイバー空間をめぐる脅威の情勢等について
（図２、３共通）

（２）IT の利活用による新しい価値の創造への対応

- **IoT やビッグデータ、AI など、IT を利活用し、新しい価値を創造するような、いわばビジネスにおけるイノベーションの実現が求められている中、サイバーセキュリティは、従来の企業内の業務の効率化によるコスト削減を目的とした IT の利活用におけるそれと異なり、事業そのものへの理解や事業のスピード感に合わせた積極的な取組が求められている。また、サイバーセキュリティの範囲も、企業の情報システム管理に関わる部門だけでなく、製造を含む事業や法務に関連する部門など分野が広がっている。**
- **このため、経営層においては、ビジネス上の「挑戦」とそれに付随する「責任」としてのサイバーセキュリティについて判断することが求められるとともに、企業内の幅広い部門を対象として、実務者層を指揮する橋渡し人材層の役割が重要となっている。また、実務者層についても、サイバーセキュリティ技術の専門家だけでなく、多様な役割を持つ関係者がサイバーセキュリティの素養を持ち、チームとなって、サイバーセキュリティを実現していくことが求められている。さらに、こうした人材育成の実施においては、産学官が人材像を共有し、連携できる仕組みを強化していくことが重要である。**

① IT の利活用の広がり（「費用」から「投資」へ）

IT の急激な進化により、サイバー空間は、実空間における人間の行動を大いに拡張し、社会・経済の構造を変え、既存の産業構造や技術分野の枠にとらわれることなく新たな価値を生み出す経済成長のフロンティアとなっている。実際、図４に示すように、IT の利活用により新たな価値の創出に取り組む企業は増加傾向にある。

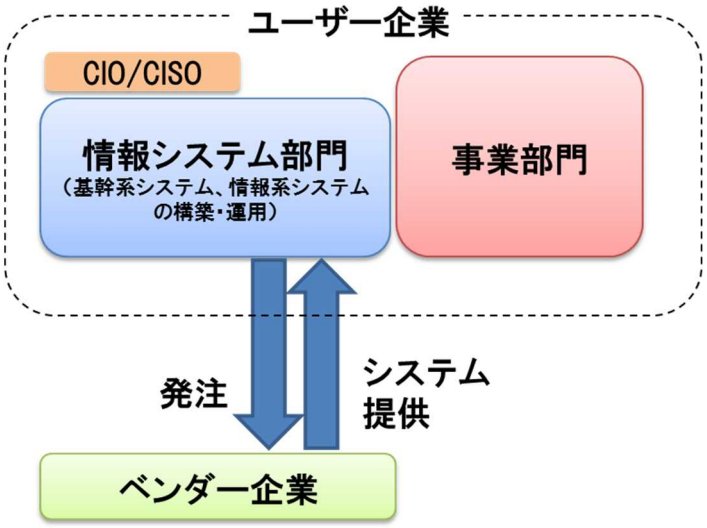


（図４）IT を活用した新しい商品、サービスの創出に関する取組状況について

出典：一般社団法人 日本情報システム・ユーザー協会 第 22 回企業 IT 動向調査 2016（2015 年度調査）

企業における IT の利活用について、従来は、図５に示すように、企業内部の業務

効率化によるコスト削減等を目的として、ユーザー企業の情報システム部門がベンダー企業から基幹系システム（生産・販売、会計、人事、給与、資産の管理等に関する企業内のシステム）や情報系システム（メールや文書作成、スケジュール管理等に関するシステム）を調達し、調達したベンダー企業に依存しつつ運用することが一般的とされてきた。この場合、ユーザーのシステム運営に関するニーズは比較的明確であり、一定の期間（数年単位）にわたって変化が少ないことが多い。情報システム部門の実務者層は、ベンダー企業と連携して、調達したシステムのサイバーセキュリティに焦点を当ててきた。



（図５）従来型の IT の利活用における体制例

- 業務効率化によるコスト削減等を目的に、情報システム部門がベンダー企業から基幹系システムや情報系システムを調達。

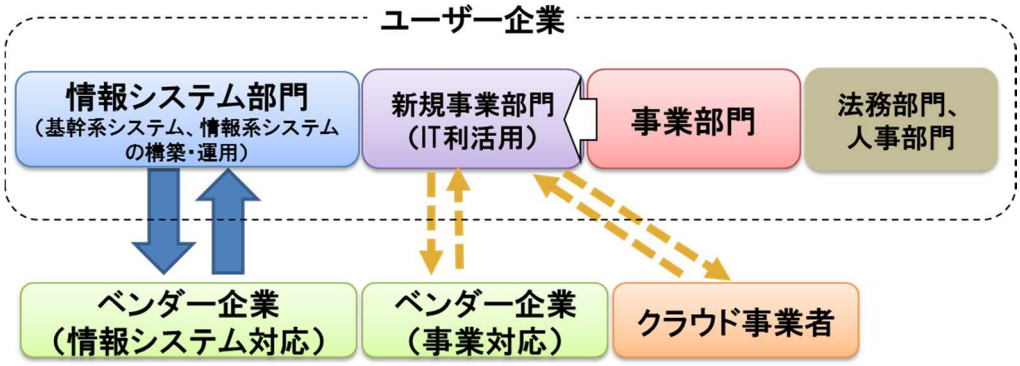
近年、経済・社会活動の大部分がインターネットに代表されるコンピュータネットワークで処理されるようになり、商品やサービスの取引形態が大きく変化するなど消費者向けのビジネスは一変した。さらに、企業間取引の世界も変革されようとしている。企業においては、グローバルに競争環境が変化していく中で勝ち抜いていくために、企業内部のコスト削減のための IT の利活用にとどまらず、IoT やビッグデータ、AI など、IT を利活用し、新しい価値を創造するような、いわばビジネスにおけるイノベーションを実現することが求められている。これには、新しいビジネスのみならず、既存のビジネスを IT の利活用により、劇的にそのモデルを改革するようなものも含まれる。例えば、IoT と AI の組み合せによって、製品は、製品単体の価値だけでなく、その「稼働」をサービスとして売ることができる可能性がある。また、機械学習によってサービスの品質が高まり、それによってサービスの価格を高めることも期

待できるようになる。さらに、その製品が置かれるオフィス、住居、商業施設、工場、農場などにおいて取得するデータや、製品が提供するサービスを起点として、それを取り巻く人々の活動やお金の流れなどを変え、事業を広げられる可能性がある。これは従来の製品単体の販売とは全く異なるビジネスモデルといえる。このような、新しい IT を利活用した「挑戦」においては、ビジネスのスピード感と一体となったシステム構築・サイバーセキュリティが求められる。いわば、サイバーセキュリティをやむを得ない「費用」ではなく、より高いレベルのセキュリティ品質を実現することにより、ビジネスにおいて新しい価値を創造し、企業価値や国際競争力を高めていくための「投資」と見ていく必要がある。このため、従来型のシステムの構築・運用と同じ考え方や体制では、サイバーセキュリティの対応が困難となりつつある。

② ユーザー企業とベンダー企業の役割の変化

新しい IT を利活用した「挑戦」においては、従来型の IT の利活用とは異なり、図６に示すように、ユーザー企業の事業の多様なニーズとその変化に素早く応えていく必要がある。すなわち、システムの構築・運用に関係する実務者層は、事業に対する深い理解や、事業を取り巻く状況の変化に対応できる高い柔軟性が求められる。また、決まったベンダー企業とだけ連携していればよいものではなく、自社の経営層や事業そのものに関わる部門はもちろんのこと、IoT やビッグデータ、AI をはじめとする高度な情報技術を持つ他の企業やクラウド事業者、さらには一般消費者を含む顧客など、多種多様なステークホルダーとの連携も求められる。さらに、事業に関わる IT は、急速に多様化・高度化しており、これまで以上に IT に関わるビジネスモデルは早く陳腐化する可能性がある。こうしたより複雑な状況の中で、サイバーセキュリティの確保に向けた取組が求められており、従来型の IT の利活用に係る知識や能力、業務姿勢でサイバーセキュリティに取り組むことは適切ではないケースが多い。

また、ベンダー企業においても、情報システム部門向けの基幹系・情報系システムの提供にとどまらず、事業そのものに関する情報システムの提案が期待されるようになっている。こうした中で、ユーザー・ベンダー企業間の人材の移動や、ベンダー企業自らが、これまでユーザー企業が行っていた事業そのものに参画するなど、従来の IT の利活用ではなかった動きが起こっている可能性がある。



（図６）新しい IT の利活用における体制例（１）

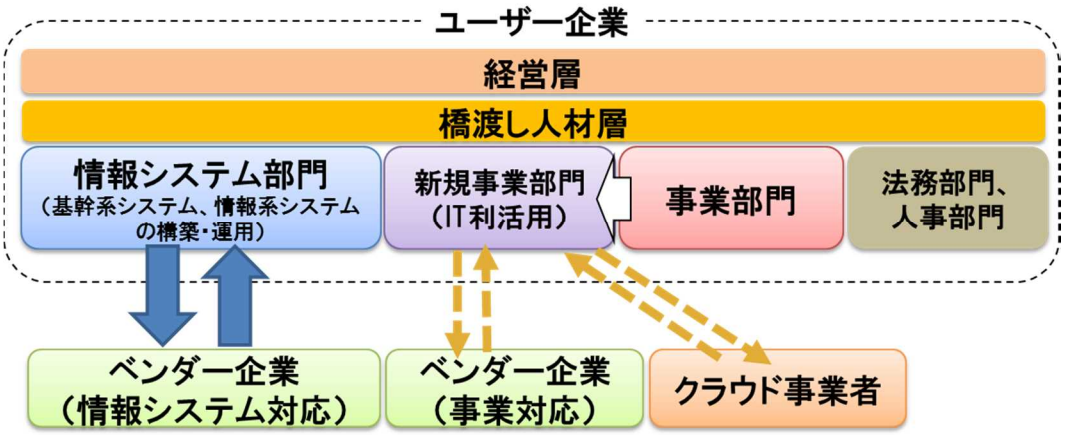
- IoT やビッグデータ、AI など、IT を利活用して新しい価値を創造するような新規事業（ビジネス・イノベーション）を立ち上げる場合、ビジネスの中核を担う事業部門がサイバーセキュリティに取り組む必要がある。
- なお、情報システム部門は社内向けの組織であり、新規事業部門は、社外向けの事業遂行組織を想定している。また、ここでは便宜上「新規事業部門」としているが、既存の「事業部門」内で、IT の利活用により新しいビジネスモデルによる事業を行う場合も含む。

③　セキュリティの範囲の広がり（経営の一項目としてのサイバーセキュリティ）

サイバー攻撃によって、個人情報や先端技術に関する情報の漏えい、インフラの供給支障といった問題、さらには IoT 機器などが攻撃の踏み台となって他者のシステムを攻撃するなど、様々な問題が起こっている。こうした攻撃に遭ってしまった企業は、サイバー攻撃の被害者である一方で、意図せず加害者側になってしまうリスクが発生し、管理責任を問われるおそれがある。こうした責任による影響として、企業は損害賠償や企業イメージの悪化、信用の毀損などが挙げられるが、企業経営の観点からは、これらは経営上のリスクであることから、サイバーセキュリティの問題は、企業経営に関わる問題といえる。また、こうしたリスクへの対策を行う上で、例えば、サイバー攻撃を防ぐのに十分な対策が行われていたこと（いわゆる善管注意義務）を証明できるようにサイバーセキュリティ対策を講じているか、あるいは、リスク評価を行う際に、リスクの認知とその対応について十分に説明できるような形で実施できているか、といった点は、法的対応の観点からも重要な課題であり、適切な監査で確認を行うことが期待される。さらには、グローバルに事業を展開する企業の場合、海外からの訴訟リスクは常にあり、その対応、特に米国の eDiscovery[1]への対処における弁護士・依頼者間秘匿特権の確保等において、法務部門も主体的に参画し、必要に応じて外部弁護士の法的アドバイスを得るなどの工夫が考えられる。加えて、有価証券報告書やコーポレートガバナンス報告書、情報セキュリティ報告書などを通じた、自社の

[1] Electronic Discovery（電子的証拠開示）：米国連邦民事訴訟において、訴訟に関連する証拠のうち、電子メールなどの電子的に保存されている情報に関するものを、相手の要請に基づき、自ら開示する手続。

リスクに関する情報発信や、自社の事業に関するセキュリティの品質をブランド価値として位置づけ、発信をする場合には、経理部門や経営企画部門といった IR 関係部門[2]、広報部門などとの連携も必要になる。このように、サイバーセキュリティのリスクマネジメントにおいて、経営層は、サイバー攻撃から技術的にシステムを保護すれば良い、情報システム部門に閉じた問題である、と捉えるのではなく、様々な部署が関わりながら、多角的にアプローチすることが求められている（図７）。



（図７）新しい IT の利活用における体制例（２）

- 多様な役割においてサイバーセキュリティの素養を持った人材が必要。
- 経営層のリーダーシップによる体制の下で、橋渡し人材層が様々な部署の実務者層を指揮しつつサイバーセキュリティを推進することが必要。

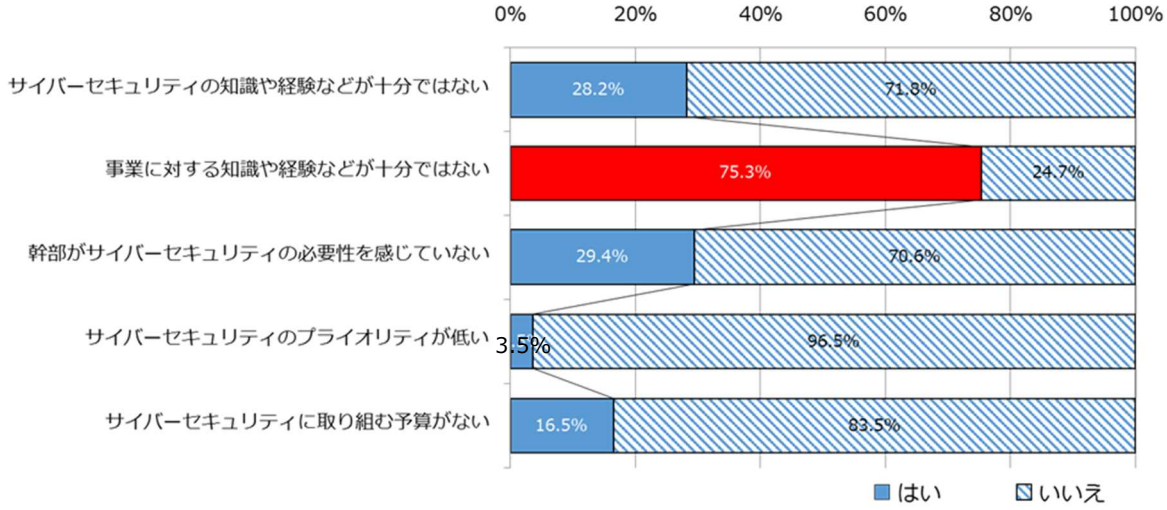
④ チームとしての対応の必要性

新しい IT の利活用におけるサイバーセキュリティ対策については、情報システム部門の人材が、事業部門のニーズを意識しつつ、事業の状況に応じて柔軟に、多様なステークホルダーを調整しつつ関連する情報システムの企画、開発、運用の支援を行うこと、あるいは、事業部門の人材が、事業そのものの企画、運用と併せてサイバーセキュリティ対策を行うことが理想的である。しかしながら、多くの場合、情報システム部門には、事業自体を理解し、事業部門に貢献する形で、サイバーセキュリティ対策に関する企画ができる人材が不足している。一方、事業部門をはじめとする組織においては、サイバーセキュリティに対する問題意識や理解が乏しい可能性がある。こうしたそれぞれの組織には長所、短所があり、組織の規模や事業内容にもよるが、例えば、単に一人だけ事業部門にサイバーセキュリティに詳しい人材を置くといった対応では解決しない可能性もある。

こうした問題に加え、先述のセキュリティの範囲の広がりを踏まえれば、従来の情報システム部門のセキュリティ担当にとどまらず、事業部門や法務部門など、多様な

[2] 財務状況や経営状況等に関する情報を発信する活動（Investor Relations, IR）に関係する部門

役割においてサイバーセキュリティの素養を持った人材の確保が必要になる。さらに、こうした人材に求められるサイバーセキュリティに関する知識や能力はそれぞれの業務における役割によって異なっており、一人で全てを解決することは適切ではないことが多い。このため、様々な役割を担うサイバーセキュリティの素養を持った人材がチームとなってサイバーセキュリティの問題に対応する体制の構築を推進することが必要となっている。



（図８）新しい IT の利活用において求められるスキル

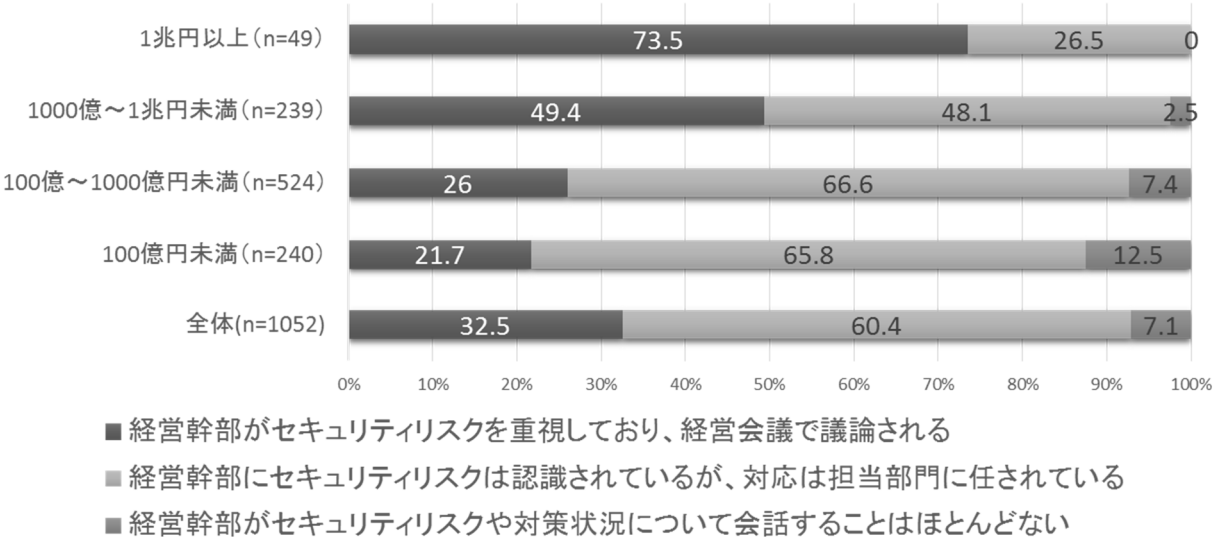
出典：NISC による日経 225 に対するアンケート調査（本質問に対する回答数は 85）

- 事業部門において IT を利活用して「挑戦」する際のサイバーセキュリティを情報システム部門が担う際に抱えている課題として、75%の企業が事業に対する知識や経験が十分ではないと回答。

⑤ 経営層の理解に関する課題

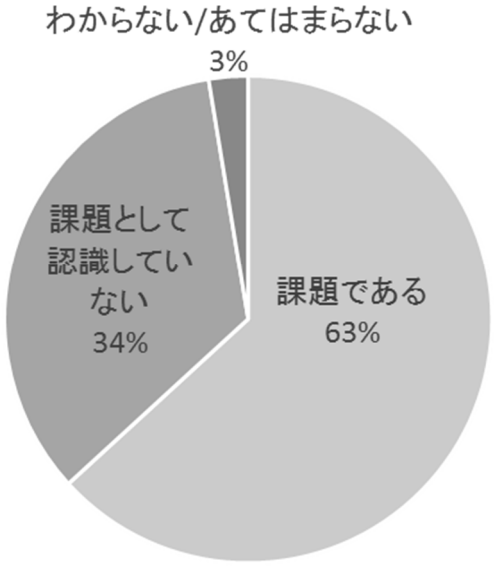
IoT システムを取り入れるなど新しい IT の利活用を推進していく中で高いレベルのセキュリティ品質を実現していく取組は、企業価値や国際競争力の源泉となる。このため、サイバーセキュリティは、利益を生み出し、ビジネスモデルを革新するときの不可欠な構成要素となるものであり、新しい製品やサービスといった価値を創造するための戦略の一環として考えていく必要がある。同時に、全てがつながる社会において、サイバーセキュリティに取り組むことは社会的な要求・要請であり、自社のみならず社会全体の発展にも寄与することとなる。このため、こうした企業における「挑戦」と、それに付随する「責任」としてのサイバーセキュリティ対策をどのように進めていくかは、企業の経営層が取り組むべき事項である。この点について、調査によれば、大企業を中心に経営層のサイバーセキュリティリスクに対する関与は高まっているものの（図９）、経営層の理解や対策の推進については引き続き課題となっていると考えられる（図 10）。さらに、情報システム部門のサイバーセキュリティ技術の専門家にとどまらず、組織横

断的に様々な役割を持った人材の指揮を伴うことからも、経営層の理解とリーダーシップが必要となっている。



（図９）サイバーセキュリティと経営者の意識

出典：一般社団法人　日本情報システム・ユーザー協会 第 22 回企業 IT 動向調査 2016
（2015 年度調査）

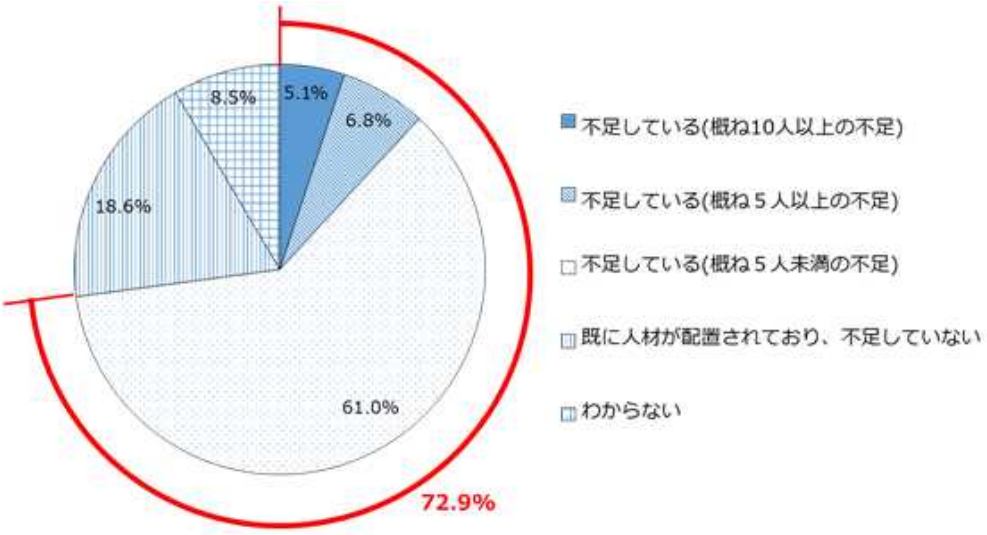


（図 10）経営層のサイバーセキュリティに対する理解と対策の推進に関する課題認識

出典：NISC による日経 225 に対するアンケート調査（本質問に対する回答数は 114）

⑥　経営層と実務者層の橋渡し役に関する課題

経営層が、新しい IT を利活用する「挑戦」とそれに付随する「責任」として、サイバーセキュリティを経営戦略の一環として認識し、位置づけたとしても、具体的にどのようにサイバーセキュリティをビジネスに位置づけ、取り組んでいけばよいかについて、経営層自らが企画・立案し、実務者層を動かすことは困難である。むしろ、経営層の補佐的な役割を担う人材が、サイバーセキュリティの素養を持ち、経営戦略だけでなく、サイバーセキュリティの関係する業務課題を十分に理解した上で、経営層に対しセキュリティに関する課題と対応を経営層に進言するとともに、技術者をはじめとする様々な役割を持った実務者層を指揮することができるいわゆる「橋渡し人材層」が必要であり、その確保が課題である（図 11）。加えて、「橋渡し人材層」がその役割を十分に遂行できるよう、「権限」と「責任」を明示する必要がある。



（図 11）橋渡し人材層の必要性

出典：NISC による日経 225 に対するアンケート調査（本質問に対する回答数は 59）

- 橋渡し人材が必要だと認識している企業（日経 225 の調査において、全体の約６割）のうち、７割の企業は不足しているとの認識。

⑦　人材像に関する共通認識の醸成と産学官の連携強化に向けた仕組みづくり

現在、産学官のそれぞれにおいて、様々なサイバーセキュリティ人材育成の取組が行われている。こうした取組の実施においては、今後、産業界において必要となるサイバーセキュリティ人材の人材像や規模について、産学官の認識が共有されていることが重要である。また、その人材像については、将来のキャリアパスが考慮されたも

のであることが不可欠である。例えば、平成 28 年９月に産業横断サイバーセキュリティ人材育成検討会において、情報システム部門を中心としたサイバーセキュリティ人材に必要とされる人材像の定義について報告書が出されている[3]。国や大学・高等専門学校はもちろんのこと、人材育成をビジネスとして行う民間企業においては、教育・訓練などの具体的な取組において、必要とされる人材像の変化にも応じつつ、このような産業界からの発信を踏まえたものとすることが重要である。加えて、人材育成に関する官民の正しい役割分担の検討や、具体的な教育・訓練プログラムの内容の検討において、産学官の連携の強化や、IT の利活用による新しい価値の創造への対応を視野に入れた知の集積を推進することが必要である。

（３）将来を視野に入れた課題（イノベーションのツールとしてのサイバーセキュリティ）

- **ビジネスイノベーションの「ニーズ」に対応したサイバーセキュリティ人材に加え、ビジネスイノベーションに対する「シーズ」を生み出せるような高度なサイバーセキュリティ人材の確保が必要である。**
- **また、サイバーセキュリティを担う人材は、イノベーションの成果を活用しつつ、課題に対して柔軟かつ積極的に対応できるような基礎力を身に付けておくことが重要である。**
- **セキュリティマインドを早期から持ち、役割に応じて対策を考えられることが必要である。このため、若年層の教育も含め、サイバーセキュリティ向上へのモチベーションを持つような人材育成に取り組むことが重要である。**

① ビジネスにおけるイノベーションに貢献できる人材の重要性

先述の通り、これまでは主に業務効率化によるコスト削減を目的とした IT の利活用が中心であったが、IoT やビッグデータ、AI などに代表される IT の利活用によって新しい価値を創造するビジネスにおけるイノベーションの実現が求められている。我が国の産業競争力を強化していく観点からも、こうしたビジネスにおけるイノベーションからの「ニーズ」に応じてサイバーセキュリティ対策ができる人材の育成が必要である。同時に、ビジネスのイノベーションにつながるような革新的なサイバーセキュリティ技術を生み出す人材、換言すれば、ビジネスイノベーションに対する「シーズ」となるサイバーセキュリティ技術を生み出せるような高度なサイバーセキュリティ人材の確保が必要である。例えば、公開鍵暗号方式（相手には公開鍵を伝え暗号化して送信をしてもらい、対となる秘密鍵で復号する方式。）の発明により、正規の受

[3] サイバーセキュリティ人材に関する試算結果については、産業横断サイバーセキュリティ人材育成検討会（平成 28 年９月発表）が業務内容に即した理想的な人材の配置を想定した試算を行っている。また、アンケート調査による現状認識を基にした試算として、独立行政法人情報処理推進機構（IPA）（平成 24 年４月発表、平成 26 年７月に追加分析を発表）や経済産業省（平成 28 年６月発表）が行ったものがある。

信者のみ安全に情報を得ることができる仕組みが実現し、電子商取引の発展などに大いに貢献したとされている。また、近年では、サイバーセキュリティに AI を活用することで、セキュリティ監視や、大規模なシステムにおけるデジタルフォレンジック（データの保全・復元・解析）、脆弱性検査などの労働集約的な業務が自動化する技術の研究が進んでいる。こうしたイノベーションにより、サイバーセキュリティ対策のコストが削減されるとともに、人間の不安定性（例えば、サイバーセキュリティの専門家の能力の違いによる対策のばらつき、判断ミス）に影響を受けにくい方向に進む可能性がある。

このように、ビジネスのイノベーションに貢献できるサイバーセキュリティ人材を確保することによって、我が国の産業競争力強化につなげていくことが期待される。

② イノベーションに柔軟に対応できる人材の重要性

ビジネスモデルのイノベーションやサイバーセキュリティ技術におけるイノベーションによって、守るべき対象や守るための方法などサイバーセキュリティの考え方が大きく変化する可能性があるため、既存の知識だけではサイバーセキュリティの向上が困難になる可能性がある。また、サイバーセキュリティの向上を実践するような AI が登場した場合、一部のサイバーセキュリティ人材の業務は AI が担うことができる可能性もある。将来を担う若い世代が、その先数十年にわたって、社会で活躍することを想定すれば、こうしたイノベーションが起こったとしても、イノベーションの成果を活用しつつ、サイバーセキュリティの課題に対して柔軟かつ積極的に対応できるだけの必要な基礎力を高めておくことが重要であり、そのようなカリキュラムを開発することが必要である。

③ サイバー空間と個人のつながり

近年、より若年の段階からますます個人がネットワークに常につながるようになっていることに加え、様々な役割の人材がサイバーセキュリティに取り組むことが求められており、サイバーセキュリティが関連する人材の裾野が広がっている。こうした中、セキュリティ技術だけに依存した対策には限界があると考えられる。むしろ、サイバー空間に関する基礎的な知識や技能を持ちつつ、セキュリティに対する意識を若年層から高めることによって、IoT を含めどのような IT の利活用であったとしても、必要なサイバーセキュリティ向上のための取組を、その時点での役割や立場に応じて考えることができるよう、サイバーセキュリティ向上へのモチベーションを持つような人材育成が必要である。

３　今後の取組方針

【基本方針】

需要（雇用）と供給（教育）の好循環の形成

＜需要＞経営層の意識改革・橋渡し人材層の配置

＜供給＞人材の量的拡大と質的向上

基本方針としては、「新・情報セキュリティ人材育成プログラム」及び「サイバーセキュリティ人材育成総合強化方針」において示した方針を踏襲するものとする。具体的には、適切な認識の下でサイバーセキュリティ人材が活躍できるような雇用とキャリアパスを確保するという人材の「需要」と、教育等を通じ、確かな知識と実践力を備え、こうした知識や能力が資格・評価基準等によって可視化され、業務経験を積み重ねることによる人材の「供給」を相応させ、好循環の形成を促進することとする。言い換えれば、まずは経営層のサイバーセキュリティに対する意識改革に取り組んでいく必要があるが、それが実現し、対策を進めようとすると、必要な知識と能力を有する人材が足りなくなるため、産学官の関係者が連携しながら、こうした課題への対応を相応させて進めていくことが重要である。

その上で、従来の業務効率化を目的とした IT の利活用だけではなく、AI など IT の利活用によって新しい価値を創造するビジネスにおけるイノベーションの実現が求められているという変化を踏まえた新たな取組が必要である。一方、サイバー攻撃の脅威の高まりを踏まえ、サイバーセキュリティ技術を担う人材の育成や、経営層の意識改革による対策の推進といったこれまでの取組は引き続き重要である。

また、これらのサイバーセキュリティに関連する人材育成の取組については、産学官連携の下、施策間連携の強化を図ることとする。

（１）状況の変化を踏まえた新たな取組

- **経営層：新たな価値の創造という「挑戦」に付随する「責任」としてサイバーセキュリティに取り組むための意識改革を図る**
- **橋渡し人材層：ビジネス戦略と一体となってサイバーセキュリティの企画・立案を行い、実務者層を指揮できる橋渡し人材層の育成に取り組む**
- **実務者層：チームとなってサイバーセキュリティを推進するための人材育成に取り組む**
- **高度なサイバーセキュリティ技術の専門性を持ち、ビジネスイノベーションが実現できる高度人材の育成に取り組む**
- **初等中等教育段階からの情報教育を充実させ、児童生徒の情報活用能力（情報セキュリティを含む）を培うことが重要**

IoT やビッグデータ、AI など、IT を利活用し、新しい価値を創造するような、いわばビジネスにおけるイノベーションが求められており、こうした「挑戦」に付随する「責任」としてのサイバーセキュリティ対策を進めていくことが重要となっている。この場合、主に業

務効率化のための情報システムのセキュリティを担ってきた情報システム部門のスペシャリストにとどまらず、経営企画部門、事業部門、製造部門、法務部門、監査部門など、企業内の幅広い組織において、それぞれの役割を担うエキスパートが対象となる。これらのエキスパートは、それぞれの役割に関連するサイバーセキュリティの素養を持ち、他の部門のサイバーセキュリティに取り組む人材やサイバーセキュリティ技術の専門人材とチームとなって業務ができるような体制を構築することが重要である。こうした認識の下、需要面と供給面のそれぞれについて、新たな取組を推進することとする。

① 需要

a. ビジネスモデルのイノベーションを生むための経営層の意識改革

先述（第２章）の通り、これまで経営層は、サイバーセキュリティをやむを得ない「費用」と見る傾向にあったが、IT の利活用の広がりを踏まえれば、より積極的な経営への「投資」と位置づけていくことが重要となっている。言い換えれば、企業の「挑戦」とそれに付随する「責任」としてサイバーセキュリティに取り組むことが必要であり、これは経営戦略そのものであるといえる。このように、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。その中で、経営層は、様々な部署の多様な役割を持った多くの実務者との調整が必要になるが、経営層が直接、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き、組織全体のサイバーセキュリティ対策を提示し、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、指揮することができる「橋渡し人材層」を置くとともに、「橋渡し人材層」がその役割を十分に遂行できるよう「権限」と「責任」を明示することが必要である。

また、企業のリスクマネジメントの観点からは、サイバーセキュリティの範囲が広がっており、従来の IT の専門部署だけにとどまらず、事業部門、製造部門、法務部門、監査部門、人事部門、広報部門など組織の中でのそれぞれの役割において、サイバーセキュリティの素養を持った人材が、チームとして連携を図りつつサイバーセキュリティに取り組む体制が必要である。

これらの課題を踏まえると、経営層がサイバーセキュリティの意識を高め、リーダーシップの下で、このような体制整備を行い、サイバーセキュリティ対策を推進していくことが重要である。

ア）企業の経営層におけるサイバーセキュリティに係る基本的な考え方の普及

NISC は、「セキュリティマインドを持った企業経営ワーキンググループ」における検討を経て、平成 28 年８月、経営層に期待される認識と、経営戦略を企画する人材層に向けた実装のためのツールを示した「企業経営のためのサイバーセキュリティの考え方」を策定した。同ワーキンググループを通じ、企業のサイバーセキュリティに係る取組について、産業界と

連携しつつ、経営層の認識や有価証券報告書をはじめとした情報発信の状況や法律・税制を含めた関連する制度面の課題等の把握に努めるとともに、シンポジウムの開催等を通じ、経営層の認識を高めていくための普及啓発を含めた推進方策等課題の解決に資する取組について検討する。

② 供給

a.　橋渡し人材層の育成の取組

「橋渡し人材層」の具体的な機能としては、自社の経営戦略や事業そのものについての深い理解と、サイバーセキュリティの素養を持つことを前提として、例えば、IoT やビッグデータ、AI など新しい IT を利用したビジネス戦略の検討と一体となったサイバーセキュリティ対策について企画・立案[4]し、経営層の理解を得て、技術者をはじめとする様々な役割を持った実務者層を指揮することができること、いわば、企業の経営戦略上必要なサイバーセキュリティ対策の「プロデューサー」として活躍できることである。こうした橋渡し人材層は、日々変化をしているビジネスモデルに関連するサイバーセキュリティの知識について、自らの学習だけでなく、組織を越えた連携等による手段で、高めておくことが期待される。このため、以下の取組を推進する。

ア）橋渡し人材層を対象とした知識・能力向上の機会の創出

橋渡し人材層は、IoT やビッグデータ、AI など IT を利用した新しい価値の創出など経営・事業戦略的な視点を持ちつつ、最新のサイバーセキュリティに関する知識・能力の向上が必要である。こうした機会を作るため、企業を越えた橋渡し人材層の連携を促進し、定期的にセミナー等の開催を行う。

イ）資格保有者を活用した橋渡し人材層の育成

情報処理安全確保支援士（通称、登録セキスペ）は、サイバーセキュリティについて高度な知識、技能を有する者であり、その業務は、自らがサイバーセキュリティに関する調査、分析、評価を行うことのみならず、それらについての相談及び助言を行うことが含まれる（情報処理の促進に関する法律（昭和 45 年法律第 90 号）第６条)。当該資格保有者の持つサイバーセキュリティに関する知識・技能を活用しつつ、経営や事業に対する知識や、情報セキュリティ監査などの経営に助言できる応用技術を身に付けることにより、橋渡し人材層の育成に貢献することが期待される。

ウ）学び直しを通じた人材の育成

橋渡し人材層が、サイバーセキュリティの知識や能力を身に付けられるよう、橋渡し人

[4] 「企画・立案」には、経営戦略や事業戦略に即したセキュリティ対策かどうか、有効性も含めて「評価」することを含む。

材層向けのモデルとなるカリキュラムの構築や、サイバーセキュリティに関する教材の作成などを通じ、学び直しの機会を創出する。

b. チームとなって推進するための人材育成の取組

IT の利活用の広がりに伴い、サイバーセキュリティ対策が要求される組織が広がっている中、一つの部門が単独で、サイバーセキュリティ対策の企画・立案や運用を実現できるとは限らない。むしろ、それぞれの組織の役割を持った人材の長所を活かし、足りない知識や能力を補いつつサイバーセキュリティに取り組めるよう、様々な役割や能力を持つ人材が組織横断的に連携し、チームとして対策に当たることを可能とする体制の構築を推進することが重要である。具体的には、サイバーセキュリティ以外を中核とする業務に従事する人材が当該業務に関連するサイバーセキュリティについて問題意識や素養を持ち、他の部門のサイバーセキュリティに取り組む人材や、サイバーセキュリティ技術の専門人材との間でサイバーセキュリティに関わる課題や対策について議論ができることが必要である。このため、共通の基礎知識と分野特有のサイバーセキュリティの基礎知識（例えば、法務部門であれば、法令等によるサイバーセキュリティ対策の要求事項など）を身に付けられる仕組みが必要となる。さらに、こうした基礎知識を前提として、経営戦略や法令等による要求、業務の実態、予算・人材等による制約条件などに照らし、最も有効かつ実施可能なセキュリティ対策を考えられるよう、各部門の業務（業務そのものだけでなく、業務によって生み出される製品・サービスを含む）について分析を行った上で、サイバーセキュリティの視点を含めたリスクアセスメントができる人材育成を行うことが必要である。こうした人材育成を実現するため、産学官が緊密に連携し、企業、独立行政法人、大学等が様々な業務に携わっている社会人向けのサイバーセキュリティに関する学習コンテンツを作成するなど、意欲ある社会人のための学びの場を形成し、キャリアパスを確立していくことが重要である。

こうした人材育成に当たっては、従来の業務効率化を目的とした IT の利活用に必要なサイバーセキュリティの知識だけでなく、企業間を含めたジョブチェンジも視野に入れた「基礎力」の高いハイブリッド型の人材育成の視点を持つような内容としていくことが重要である。加えて、教育の質を高めていく観点からも、製造分野（例：制御システムや自動車）や法律分野など様々な分野に関わるサイバーセキュリティについて、知の集積などを通じ、学問領域として確立していくことも重要である。こうした方向性の下、以下の取組を推進する。

ア）様々な役割を担う社会人の「学び直し」を通じたセキュリティのスキル向上

これまで、必ずしもサイバーセキュリティを中核とした役割を担ってこなかった人材を含めて、セキュリティの知識や能力を高め、チームとなってサイバーセキュリティ対策ができるよう、社会人の「学び直し」の機会の創出を推進する。

具体的には、文部科学省における「成長分野を支える情報技術人材の育成拠点の形成

（enPiT）」の実施において、大学が有する最新の研究の知見に基づき、拠点大学を中心とした産学教育ネットワークを構築し、社会人を対象とした情報技術人材育成のための短期の実践的な学び直しプログラムを開発・実施する。

また、経済産業省所管の独立行政法人情報処理推進機構（IPA）における産業サイバーセキュリティセンターにおいて、企業で自社のセキュリティ対策の中核を担う人材が、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用い、専門家と共に安全性の検証や早期復旧等の実践的な演習を繰り返し行う。これにより、実践経験を身に付けるとともに、他の企業・業界の受講生や指導を担う高度な能力を持つ国内外の専門家等との人脈形成を通じ、重要インフラ・産業基盤のサイバーセキュリティ対策の根幹を担う人材育成を推進する。

さらに、戦略的イノベーション創造プログラム（SIP）の「重要インフラ等におけるサイバーセキュリティの確保等」（平成 27 年度～31 年度）のうち、セキュリティ人材育成の事業において、重要インフラ事業者の運用技術者に必要なサイバーセキュリティの知識・スキルを育成するため、カリキュラムの研究開発を実施するとともに、その成果の普及に取り組む。

イ）高等専門学校おける情報系学科の学生にとどまらない教育の推進

高等専門学校において、情報系学科の学生のみならず、その他の専門分野（機械や電気など）の学生も含め、企業と連携したサイバーセキュリティのスキルセット（到達目標）の構築、教材開発、情報セキュリティの教育実践と到達度評価に加え、実践的な演習環境を整備することにより、それぞれの専門分野における秀でたサイバーセキュリティの素養を持った人材の発掘・育成を図る。

ウ）様々な役割を持った実務者層におけるセキュリティのスキルの評価

情報システムの各利用部門におけるセキュリティ担当者（実務者層）の、業務を踏まえたリスクアセスメント能力や、業務遂行に必要な情報セキュリティ対策について目的や内容を適切に理解する能力、対策を実装する技術者とスムーズにコミュニケーションができる能力等を適切に評価できるよう、「情報セキュリティマネジメント試験」の活用を促す。

c. 高度人材（セキュリティ技術のイノベーション人材）の育成

新しい IT の利活用によるビジネスイノベーションに伴うリスク対応の「ニーズ」に応じてサイバーセキュリティの向上ができたり、ビジネスイノベーションに対する「シーズ」となるサイバーセキュリティ技術を生み出せたりするような高度なサイバーセキュリティの技術を持つ人材の確保が必要である。

こうした高度人材は学校や企業などの組織が用意した人材育成のカリキュラムや資格等を通じて育成するだけでは不十分である、むしろ、「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”づくりの推進が重要になってくる。また、その際、グローバル水準における自らの位置を把握でき、モチベーションを高めることができるような形で実施することが重要である。このため、以下の取組を推進する。

ア）若手のセキュリティエンジニアの発掘・育成

総務省所管の国立研究開発法人情報通信研究機構（NICT）に組織された「ナショナルサイバートレーニングセンター」において、若年層の ICT 人材を対象に、高度なセキュリティ技術を本格的に指導し、未来のサイバーセキュリティ研究者・起業家の育成に取り組む。

d. 初等中等教育段階における情報教育の充実

社会において活躍するセキュリティ人材の裾野が広がっていることを踏まえれば、初等中等教育段階からの情報教育を充実させ、児童生徒の情報の科学的な理解[5]に裏打ちされた情報活用能力（プログラミング的思考[6]や情報セキュリティ、情報モラルを含む）を培うことが重要である。その際、教員についても、こうした取組に関する指導力の向上を目指した研修等の改善・充実を進めることが重要である。このため、以下の取組を推進する。

ア）児童生徒の発達段階に応じた情報活用能力（プログラミング的思考や情報セキュリティ、情報モラルを含む）の育成

文部科学省においては、教科横断的な情報活用能力の育成に係るカリキュラム・マネジメントの在り方や指導方法等について実践的な研究等を実施する。

（2）これまでの取組の充実

- **中小企業も含めて、実務者層だけの問題ではなく、経営問題としてサイバーセキュリティ対策を捉えるよう、引き続き意識改革を推進する。**
- **サイバー攻撃の脅威の高まりや企業統合に伴うセキュリティの必要性、2020 年東京オリンピック・パラリンピック競技大会等を見据え、サイバーセキュリティ技術に関する知識・能力を向上するための取組や、高度な情報セキュリティ技術の専門性を持った人材の発掘・育成についても、充実を図る。**

[5] 情報活用の基礎となる情報手段の特性と、情報を適切に扱ったり、自らの情報活用を評価・改善するための基礎的な理論や方法の理解（平成 22 年 10 月 文部科学省「教育の情報化に関する手引」）

[6] 自分が意図する一連の活動を実現するために、どのような動きの組合せが必要であり、一つ一つの動きに対応した記号を、どのように組み合わせたらいいのか、記号の組み合わせをどのように改善していけばより意図した活動に近づくのか、といったことを論理的に考えていく力（平成 28 年 6 月 16 日　小学校段階における論理的思考力や創造性、問題活用能力等の育成とプログラミング教育に関する有識者会議「小学校段階におけるプログラミング教育の在り方について（議論のとりまとめ）」）

これまで、主に業務効率化のための企業内の情報システムを対象として、標的型攻撃による情報漏えいなどを想定したサイバーセキュリティ技術に関する深い知識と実践力を持つ専門人材の育成が重要であるとの認識の下、取組を進めてきた。人材育成の主な対象としては、IT ベンダーやセキュリティベンダー、ユーザー企業の情報システム部門のセキュリティ人材である。こうした人材に関する需要（雇用）については、経営層の意識改革等に向けた取組が進展するとともに、供給（教育）については、スキル標準[7]や様々な教育プログラムや演習の機会などが整備されてきており、着実に成果を挙げてきているといえる。一方、サイバー攻撃の脅威が高まっていることに加え、企業の統合に伴うセキュリティに関する対応の必要性やサプライチェーンにおけるサイバーセキュリティの問題、さらには、2020 年東京オリンピック・パラリンピック競技大会に向けたサイバーセキュリティ人材の育成の重要性などを踏まえ、これまでの人材育成の取組の充実を図っていくことが重要である。また、産業界においては、経営層の関与を高めることを目的として業種横断的に経営層が集まる機会を設けることや、産学連携による実践的なセキュリティ教育（産学連携講座、寄附講座等）の実施、インターンシップの受入れなどの取組が期待される。さらに、企業活動がグローバル化していることを踏まえ、海外におけるサイバーセキュリティ人材の育成も重要な課題となっている。このため、こうした我が国における人材育成の課題に取り組むことで得られた知見を活かし、海外におけるサイバーセキュリティ人材の育成に貢献することも重要である。

① 需要

a. サイバーセキュリティ対策における経営層の意識改革

サイバーセキュリティの水準を自組織の要求事項に適合するよう経営資源を投じるとともに、サイバーセキュリティ対策が必要な部署への人材の配置を図るため、経営層は、実務者任せにすることなく、経営戦略の一環としてサイバーセキュリティ対策を位置づけることが重要である。このため、経営層の意識改革に向けたこれまでの取組を継続する。また、中小企業をはじめ自らセキュリティ対策を行う上で、事業上のリソースの制約が大きい企業については、外部の能力や知見を活用せざるを得ないと思われる。このため、中小企業の経営者のサイバーセキュリティに関する意識啓発を図りつつ、サイバーセキュリティの確保に貢献できる地域の人材育成など、引き続き、中小企業の対策に資する環境整備を推進する。

ア）サイバーセキュリティ経営ガイドラインの普及

企業の経営層が認識すべきサイバーセキュリティに関する原則やリーダーシップが必要

[7] スキル標準の例として、IPA は、会社の業務を見える化し、潜在的な問題発見とソリューション、必要な人材を明確化するために「i コンピテンシディクショナリ」を策定している。また、JNSA（特定非営利活動法人日本ネットワークセキュリティ協会）は、情報セキュリティに関する業務に携わる人材が身に着けるべき知識とスキルを体系的に整理した情報セキュリティ知識項目（SecBoK）を整理している。

な項目の理解の促進を図るため、経済産業省は、IPA とともに、平成 27 年 12 月、経営者が認識すべき「３原則」と、経営者がサイバー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 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」を策定（平成 27 年 12 月策定、平成 28 年 12 月一部改訂）した。引き続き、企業のサイバーセキュリティ対策を推進するため、産業界と連携しつつ、セミナーでの説明やガイドラインに基づく各社の取組の紹介などを通じて当該ガイドラインの普及に取り組み、経営者の意識を高め、リーダーシップを促していくことが重要である。さらに、「重要インフラの情報セキュリティ対策に係る第４次行動計画（案）」を踏まえ、内閣官房及び重要インフラ所管省庁は、重要インフラ事業者等の経営層に対して情報セキュリティに関する意識を高めるように働きかけを行う。[8]

イ）中小企業のサイバーセキュリティ対策の普及啓発に向けた取組

IPA は、中小企業の経営者がサイバーセキュリティ対策の必要性を認識し、自らの責任で対応しなければならない事項について解説し、簡単に自社のセキュリティが診断できるツールを提示した「中小企業の情報セキュリティ対策ガイドライン」を策定している（平成 21 年策定、平成 28 年 12 月改訂）。引き続き、こうしたコンテンツを活用し、中小企業団体等と連携を図りつつ、中小企業の経営者の意識改革をはじめとしたセキュリティ対策の普及啓発に取り組むことが重要である。

② 供給

a. サイバーセキュリティ技術に関する知識・能力を高めるための取組

セキュリティを専門とする技術者、さらには、情報システムの設計・開発・運用に携わる技術者のサイバーセキュリティ技術に関する知識・能力を高めることが重要であるとの認識の下、これまで、関係各省や業界団体等の各主体により積極的な教育・啓発活動が行われてきた。加えて、サイバーセキュリティ人材の能力を評価し、それを組織内での業務・処遇等に反映させていくため、評価基準・資格等の整備が進められてきた。2020 年東京オリンピック・パラリンピック競技大会に向け、セキュリティ人材の確保の観点から、引き続きこれらの施策を推進することが重要である。

ア）情報セキュリティのスキル向上のための実践的取組の実施

サイバー攻撃に対する防御を行うためには、実際にどのような手口でサイバー攻撃が行われ、それに対してどのような防御を行ったらいいかといった実践的な知識が重要である。このため、国の行政機関、地方公共団体、独立行政法人、重要インフラ事業者等を

[8] 「重要インフラの情報セキュリティ対策に係る第４次行動計画（案）（平成●年●月●日）」においては、「内閣官房及び重要インフラ所管省庁は、重要インフラ事業者等の経営層に対して情報セキュリティに関する意識を高めるように働きかけを行うとともに、そのような働きかけを通して知見を得て、重要インフラ防護施策を実態に即した実効的なものとする。」としている。

対象として、実践的サイバー防御演習（CYDER）（平成25年度より総務省が実施、平成28年度よりNICTが実施主体となっている）を実施してきたところ、引き続き実施していくことが重要である（平成29年度からは、NICTに組織された「ナショナルサイバートレーニングセンター」において実施）。なお、こうした演習や、民間や大学における演習の実施については、組織内の様々な役割を持った担当者がチームとなってインシデントの対応に当たることを想定した、実践的なものであることが重要である。

イ）評価基準としての資格等の整備

国家資格の情報処理安全確保支援士（登録セキスペ）制度を創設（平成28年創設）し、最新のサイバーセキュリティに関する知識、技能を有する専門的な者を有資格者として認定する仕組みが開始されたところであり、2020年までに３万人の登録者数を目指している。今後、同国家資格を活用しつつ、情報処理技術者を育成し、企業等の情報システムのサイバーセキュリティを担う人材を確保していくことが重要である。

ウ）大学の知見を活用した情報セキュリティ技術人材の育成

文部科学省の「職業実践力育成プログラム」（BP）認定制度によって、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大臣が認定しており、認定コースとして、例えば、平成27年より、東京電機大学において、国際化サイバーセキュリティ学特別コース（CySec）がスタートしている。

引き続き、こうした大学の知見を活用した情報セキュリティの技術人材の育成を推進することが重要である。

b. 高度な情報セキュリティ技術の専門性を持った人材の発掘・育成

2020年東京オリンピック・パラリンピック競技大会に向け、高まるサイバー攻撃の脅威に対する対応ができるよう、高度な専門性を持ったサイバーセキュリティ人材を発掘・育成していくことが重要である。また、こうした人材は、セキュリティ人材育成において、教育する側となることも想定されるため、難解な専門知識を分かりやすく説明する能力を高めることが求められる。

ア）大学におけるセキュリティの専門教育の充実

文部科学省における「成長分野を支える情報技術人材の育成拠点の形成（enPiT）」（平成24年度より実施）のセキュリティ分野では、５大学（情報セキュリティ大学院大学、東北大学、北陸先端科学技術大学院大学、奈良先端科学技術大学院大学、慶應義塾大学）が中心となり産業界との協働のもと、大学院修士課程の学生を主な対象として実践的なセキュリティ人材の育成を進めてきた。平成28年度からは大学連携のネットワークを拡充して学部教育における基礎的人材育成の取組も開始している。引き続き、こうした大学

における専門性を持った情報セキュリティ人材の育成や裾野の更なる拡大を推進することが重要である。

イ）高等専門学校や専修学校等における教育の推進

高等専門学校は、企業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、教材開発を行うとともに、情報セキュリティの教育実践と到達度評価、実践的な演習環境の整備を実施してきており、引き続き高等専門学校における情報セキュリティ技術の教育を行う。

また、専修学校における教育に関しては、企業等との密接な連携により、より実践的な職業教育に組織的に取り組む専門課程を文部科学大臣が「職業実践専門課程」として認定する制度（平成 25 年創設）がある。こうした制度の活用を通じ、専修学校におけるセキュリティ教育の充実を図る。

ウ）突出した能力を持つ人材の発掘・育成

IPA は、民間事業者と連携し、若年層のセキュリティ人材（22 歳以下）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のノウハウを第一線の技術者から若手に伝授する「セキュリティ・キャンプ全国大会」を実施している。この取組は平成 16 年から行われており、平成 25 年からは、地方における人材の裾野と輪を広げるため、「セキュリティ・キャンプ地方大会」も実施している。引き続き、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の創出を目指す。

エ）2020 年東京オリンピック・パラリンピック競技大会に向けた高度人材の育成

NICT に組織された「ナショナルサイバートレーニングセンター」において、2020 年東京オリンピック・パラリンピック競技大会の適切な運営に向けたサイバー演習（サイバーコロッセオ）を実施し、高度な攻撃に対処可能な高度な能力を有するサイバーセキュリティ人材の育成・組織間連携の強化を推進する。

（３） 人材育成の質を高めるための新たな取組

- **需要と供給の好循環を形成するため、NISC が中心となって、産学官の連携を図るためのネットワークの強化や、モデルとなるカリキュラムの策定をはじめ各施策間の連携強化に向けた取組を推進する。**

サイバーセキュリティ人材の「需要」と「供給」の好循環を形成していくためには、需要を生む産業界と、教育・訓練を担う独立行政法人や大学等の機関の産学官の連携の下、産学官で人材像の正しい認識が共有されていることが必要である。また、（１）の新たな取組、

（２）のこれまでの取組に関わらず、個々の施策の効果を高めるためにも、モデルとなるカリキュラムの策定をはじめとした施策間の連携強化が重要である。こうした産学官の関係者間における連携強化を促すため、NISC が中心となって以下の取組を推進する。

a. 産学官の連携を図るためのネットワークの強化

情報セキュリティ社会推進協議会をはじめ、産学官の多様な主体で構成される場を活用し、サイバーセキュリティ人材の人材像や人材育成の取組・課題等に関する情報共有などネットワークの強化を行う。

b. 各施策における連携の強化

経営層、橋渡し人材層、実務者層、高度人材、それぞれの人材層を対象に、教育・訓練や、実践的な演習、これらの人材の評価など、様々な施策が実施されている。今後、個々の施策について連携を強化することにより、より効果的な実施を図ることができるとともに、セキュリティ教育に関わる有限なリソース（例：コンテンツ作成の関係者や教育者）を効率的に活用できる可能性もある。このため、産学官からなる実務者のワーキンググループを通じ、以下の取組を推進する。

- 具体的な人材像の認識を共有した上で、モデルとなる具体的な人材育成のカリキュラムを策定
- 実践的演習の共同実施やシナリオの共有、教育プログラムにおける教材の共有
- 教育プログラムや演習への参加による試験または試験に係る講習の一部免除

４　まとめ

- これまで、我が国においては、国や民間企業、大学が、業務効率化を主な目的とした企業の持つ基幹系システムや情報系システムをサイバー攻撃から防御するためのサイバーセキュリティ技術を持つ専門人材を中心に育成に取り組んできた。サイバー攻撃の脅威が高まっている中、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、こうしたサイバーセキュリティ技術の専門人材の確保は引き続き重要な課題である。

- また、近年では、IoT やビッグデータ、AI など IT を利活用し、新しい価値を創造するビジネスにおけるイノベーションの実現が求められている。こうした中、サイバーセキュリティをビジネスのイノベーションによる「挑戦」とそれに付随する「責任」として推進することができる人材の育成を含めた体制の構築が課題となっている。そのためには、経営層のリーダーシップがこれまで以上に求められるほか、橋渡し人材層の配置・育成や、様々な役割を持った人材がチームとなってサイバーセキュリティに取り組めるようにしていくことが必要である。

- 加えて、IT の利活用によるビジネスのイノベーションにおいて、その「ニーズ」に対応したサイバーセキュリティ技術を考えられる人材や、ビジネスのイノベーションの「シーズ」となりうるサイバーセキュリティ技術を考えられる人材を発掘し、育てていくことも必要である。

- さらに、サイバーセキュリティが求められる人材の裾野が広がっていることや、技術だけに依存した対策には限界があることを踏まえ、サイバーセキュリティに対する意識を高めていくような初等中等教育を推進することが必要である。

- これらのサイバーセキュリティ人材を取り巻く課題については、適切な認識の下で人材が活躍できるような雇用とキャリアパスを確保するという人材の「需要」と、教育等を通じ、確かな知識と実践力を備え、業務経験を積み重ねることによる人材の「供給」を相応させ、好循環の形成を促進していくことが重要であるとの認識の下、これらの課題解決に資するよう産学官が連携しつつ、モデルとなるカリキュラムの策定をはじめとする施策間連携を推進することとする。

- また、引き続き、産学官の取組状況・成果や、各施策間の連携の状況・成果、サイバーセキュリティ人材を取り巻く課題については、フォローを行い、適時、必要に応じて本プログラムの見直しを検討することとする。

「サイバーセキュリティ人材育成プログラム（案）」に対する意見募集の結果の概要

資料2－3

- 実 施 方 法：　NISCのWebページ及び電子政府の総合窓口（e-Gov）に掲載して公募
- 実 施 期 間：　2017年３月13日（月）～ ３月24日（金）
- 意 見 総 数：　15者から69件 【内訳：2企業・団体から延べ13件、13個人から延べ56件。】

意見内容の内訳：

１．本プログラムの趣旨・位置づけ等に関わる意見	8件
２．本プログラムの状況の認識に関わる意見	3件
３．今後の具体的な取組に関わる意見	17件
４．資格制度に関わる意見	6件
５．その他意見	35件

意見を踏まえた修正：　全3件

注）提出された意見等は必ずしもこれらに分類されるわけではないが、事務局で理解した区分にて計上している。

意見募集に対して寄せられたご意見の概要及びご意見に対する考え方

資料2－4

※ご意見の全体像が分かるように、代表的な意見を例として抽出し、その趣旨を踏まえて編集・整理しております。

番号	具体的な意見内容	ご意見に対する考え方
1	○本プログラムの趣旨・位置づけ等に関わる意見 （意見の例） ・サイバーセキュリティ人材育成プログラムに賛同する ・情報セキュリティとサイバーセキュリティ、そしてセーフティなどのマッピング、サイバーセキュリティ人材の定義、人材育成の方向性を明確にすべき ・いつまでに、何を達成できるのかが不明。希望の持てるプランを提示いただきたい ・誰を対象にしているのかが不明。研究者・開発者や官僚の育成の観点が非常に乏しく、文書のスコープが狭すぎる ・サイバーセキュリティを経済活動の一環として捉えており、国家安全保障や治安活動を含めた視点に乏しい ・民にできる部分は民が担うよう、積極的に官から民への移行を支援すべき ・サイバーセキュリティを社内向け（守り）と社外向け（攻め）を明確に分けて考えることが重要である	本プログラムは、企業をはじめとする社会で活躍できるサイバーセキュリティに関連する人材育成の方向性を示すことにより、安全な経済社会の活動基盤としてのサイバー空間の形成に向けた環境整備を図るものです。こうした中で、ビジネスにおけるイノベーションの担い手となりうる研究者や開発者も対象とし、高度人材として記載しております。また、サイバー攻撃は、国民生活や国際社会が危機にさらされる原因となりうるとしており、こうした脅威に対処できることも人材育成の目的としております。さらに、若年層の教育も含め、サイバーセキュリティ向上へのモチベーションを持つような人材育成に取り組むことが重要であることを位置づけております。今後、サイバーセキュリティをとりまく状況や課題については、フォローを行い、適時、必要に応じて本プログラムの見直しを検討することとしております。その中で、本プログラムの趣旨・位置づけや、状況の認識等に関し、いただいた御意見を参考にさせていただきます。
2	○本プログラムの状況の認識に関わる意見 （意見の例） ・「サイバーセキュリティ人材育成の取組については一定の成果があったといえる」とあるが、エビデンスを提示いただきたい ・情報処理技術者というよりも、社会人や学生などにおいて、ITリテラシーが不足していることが問題である ・セキュリティを「投資」と考える場合、リターンを求めないリスク低減や製品・サービスの付加価値向上、ひいては競争力向上や企業価値向上を図るために必要不可欠なものが重要である	
3	○今後の具体的な取組に関わる意見 （意見の例） ・業務の規模と内容に応じて、必要なスキル（資格）を持つ人材を一定数必置とし、さらに不作為によるインシデント発生時には経営層への罰則も検討すべき ・欧州でも話題になっているように、セキュリティベンダーによるビジネスのための偏向したデータを政府がそのまま利用している。攻撃を明確にした上で、顕在化の可能性、社会的影響の大きさを検討し、何をする人材がどの程度必要かを明確にすべき ・サイバーセキュリティに特化した教育だけではなく、基礎分野の教育についても支援・強化をすべき ・日本国内の独自の認定制度に基づく官中心の人材育成ではなく、国際的に認定されている民間資格や教育プログラムも積極的に取り入れるべき ・セキュリティ対策の有効性評価は、実務部門から独立したリスク管理部門や専門知識を持った経営者が行うべき ・サイバーセキュリティを投資として考えよというのであれば、投資効果を適切に判断できる基準を示すべき ・各所・各層におけるサイバーセキュリティ人材に求められる「素養」の具体化、サイバーセキュリティ人材の新たな活躍の場への流動性を高める方策の検討を行うべき ・情報通信の基礎知識保有者として無線従事者や工事担当者の人材活用や従来の技術をカリキュラムに取り入れる議論をすべき ・セキュリティの自動化に関する技術や知見をもった人材育成に力を入れるべき ・サイバーリスクへの対応には、クラウドへの理解や語学の能力も必要 ・「産学官からなる実務者のワーキンググループ」では、産学官の各活動の相互連携や重複排除の観点が重要 ・セキュリティ技術のイノベーション、ビジネスイノベーションは、一企業が自らの予算では対応不可能なので、国としての積極的な支援をお願いしたい ・産学連携による人材育成の推進（寄附講座等の産学連携活動）も盛り込んでほしい ・初等教育に関しては、大学まで含めたトータルでの教育体系を考慮すべき ・教える側の人材育成の課題解決が必要である ・経営層の意識改革は、政府からの働きかけが重要である	需要と供給の好循環を形成するため、NISCが中心となって、産学官の連携を図るためのネットワークの強化や、モデルとなるカリキュラムの策定をはじめ、各施策間の連携に向けた取組を推進することとしております。具体的には、サイバーセキュリティ人材に関する施策間連携ワーキンググループ等を通じて、関係府省庁や産業界、大学等とも連携し、今後の具体的な取組を推進してまいります。こうした今後の活動の中で、いただいた御意見を参考とさせていただきます。
4	○資格制度に関わる意見 （意見の例） ・2020年までに3万人を確保するため、受験機会を増やしたり、同レベルの民間資格の保有者に情報処理安全確保支援士の資格を付与することを検討すべき。また、資格保有者に対するインセンティブを増やすことを検討すべき ・情報セキュリティシステムアドミニストレータの合格者を活用すべき。例えば、情報処理安全確保管理士などを創設し、情報セキュリティシステムアドミニストレータ合格者をみなし合格者とすべき ・情報システムの利用部門への普及を促す観点から、「情報セキュリティマネジメント試験」について、「情報処理安全活用推進士」等とした名称独占の国家資格を創出すべき ・情報処理安全確保支援士の配置を義務化し、一定数配置した場合には税制優遇を与えるなどの制度整備により、サイバーセキュリティ人材育成に係るメリット・デメリットを定義すべき ・情報処理安全確保支援士に関する試験免除の制度を改善すべき	
5	○その他の意見 （意見の例） ・eDiscoveryは訴訟対応であり、サイバーセキュリティとは別の領域である ・技術的修正に関する意見（西暦による表記を年号によるものにすべき等）	・本プログラムでは、セキュリティの範囲が広がっていることを解説しております。その観点で、その他の意見につきましても、今後の取組の参考とさせていただきます。 ・技術的修正に関する御意見の一部については、それを踏まえて本文の修正をさせていただいております。