サイバーセキュリティ人材育成の取組について

資料２－１

NISC

- 「セキュリティマインドを持った企業経営WG」および「サイバーセキュリティ人材の育成に関する施策間連携ＷＧ」において、企業において求められる**各層（経営層、戦略マネジメント層、実務者層・技術者層）別の人材像やキャリアパスを整理**するとともに、人材の各層に対する**各省の人材育成施策に関する全体像を整理**。

- 上記の検討を踏まえて、本年５月に**「サイバーセキュリティ人材育成取組方針」**を決定。その内容を新たな**「サイバーセキュリティ戦略」に反映**（本年７月に閣議決定）。今後は、これらに基づき施策を推進していく。

※「サイバーセキュリティ戦略」（2018年7月27日閣議決定）における記載
「（略）教育等を通じ、資格・評価基準等によって可視化された確かな知識と実践力を備えた人材が、適切な処遇を受け、更に実務経験を積み重ねることにより、人材の需要と供給が相応されるといった好循環の形成が必要である。
　このため、産学官が連携して人材の需要や人材育成施策に関する情報共有等の連携を図りつつ、人材育成・確保を強化していく。（略）」

サイバーセキュリティ人材育成取組方針
～事業継続と価値創出に向けた産学官連携の推進～（概要）

・「サイバーセキュリティ人材育成プログラム」（平成29年４月決定）、「中間レビュー」（平成29年７月決定）を踏まえ、①経営層によるリスクマネジメントの一環としてのサイバーセキュリティ対策の推進、②戦略マネジメント層の人材像や各人材層におけるモデルカリキュラム等について、それぞれ「セキュリティマインドを持った企業経営WG」（主査：林紘一郎情報セキュリティ大学院大学教授）、「サイバーセキュリティ人材の育成に関する施策間連携WG」（主査：後藤厚宏情報セキュリティ大学院大学学長）において検討を実施。
・ 本取組方針の内容を今夏策定する次期サイバーセキュリティ戦略に反映し、具体的な取組を推進。

	経営層	戦略マネジメント層	実務者層・技術者層
役割	● ビジネスやサービスの着実な遂行（任務保証）が重要 ● 事業継続と価値創出のためのリスクマネジメントの一環として、対策を推進	●事業継続と価値創出に係るリスクマネジメントを中心となって支える役割 ●経営層の方針を踏まえた対策立案、実務者・技術者の指揮	●方針を踏まえたセキュリティ対策の企画・構築・実施
課題	◆リスクマネジメントに向けた、経営層の理解と意識改革の推進 ◆業種・業態の違いを踏まえた、サイバーセキュリティの位置付けの明確化とリスクマネジメントの浸透 ◆取組に対する経営上のインセンティブ付与	◆マネジメント機能の中でサイバーセキュリティリスクを考慮する必要 ◆戦略マネジメント層向けの適切な教材やプログラムが存在しない	◆経営層・戦略マネジメント層を支え、他の専門人材とチームの一員として対処できる人材の育成 ◆新たな技術やシステム開発手法の知識・スキルの育成
	人材規模・キャリアパス（需要）と、人材育成施策（供給）の好循環		
今後の施策の方向性（産学官の連携）	**○経営層の理解と意識改革の推進** ✓経営層が果たすべき役割、認識の共有 ✓経営層向けのツールの検討 ✓経営層向け伝道師の発掘・派遣 ✓「経団連サイバーセキュリティ経営宣言」の普及 **○業種・業態別の差異を踏まえた基盤の整備** ✓業種・業態別に対策レベルを示すツールの整備 ✓企業関係法制度の整理に向けた検討 **○サイバーセキュリティ投資のためのインセンティブ** ✓情報開示の推進（ガイドラインの策定等） ✓税制優遇の執行やサイバー保険活用の検討	**○組織における戦略マネジメント層の定着** ✓ 戦略マネジメント層の意義に対する経営層の理解の推進 ✓ 戦略マネジメント層の機能の明確化 ✓ 戦略マネジメントとセキュリティ対策が調和した指針の整備 **○カリキュラム・教材開発と学び直しの推進**	**○経営層・戦略マネジメント層を支える人材育成** ✓産学官連携によるカリキュラムの検討・実施 **○クラウドや先端技術等の利用に係る人材育成** ✓先端技術等の利用に関わるセキュリティの知識・スキル育成
	○サイバーセキュリティ人材育成施策の充実・強化と施策間連携の推進 **○人材育成の「見える化」の推進** ✓ 米国の取組等を参考にしつつ、産学官連携により需要と供給の「見える化」を推進 [例] 人材規模・キャリアパスの明確化、カリキュラム・教材等が一覧になったポータルサイトの整備、育成プログラムの適切な評価基準の策定等		

若年層における教育の充実
＜課題＞ ICTの基本的な原理・仕組みなどを理解し、論理的思考力を育てるとともに、情報モラル教育も重要
＜施策＞ 初等中等教育段階での教育課程内の取組に加え、地域や企業等で、自由に機器・ツールを用いて学べる機会を創出

中小企業関連の取組
＜課題＞ 知識・スキルが十分ではなく、セキュリティ対策への投資が困難。踏み台となった場合、社会への影響が大きい。
＜施策＞ 業種毎のアプローチ、セキュアモデル（クラウド活用等）と一体の対策集の策定・普及、インセンティブの仕組（税制優遇等）の検討

※基本的には、経営層及び中小企業関連の取組については、企業経営WG、それ以外の部分は施策間連携WGの報告書に基づく。

各省庁の人材育成施策に関する全体像

総務省　文科省　経産省　金融庁　その他

対象			演習（注）	教育（注）	資格・評価基準（注）
社会人	ユーザー企業	経営層	金融庁Delta Wall Ⅲ演習（五日間/H30年）（H28年度～）【約100社/H30年】 IPA産業ｻｲﾊﾞｰｾｷｭﾘﾃｨｾﾝﾀｰ責任者向け短中期期ﾌﾟﾛｸﾞﾗﾑ（２日間～2カ月）（H29年度～）【140人/年】 大学等に対する研修・実践的な演習（H30年度～）【H30:経営層80人、戦略マネジメント層120人、CSIRT要員360人、監査担当者120人/年】（H31~拡充）	放送大学BS232ch、オンライン、面接授業（1年間）（H30年度～）【500~1000人/年】※1 放送大学BS231ch（生涯学習支援番組）（H30年度～）※2 enPiT-Pro事業による社会人向け学び直し拠点の整備（3か月～6か月）（H29年度～）【メインコース：19人/年、クイックコース：100人/年】 IPA産業サイバーセキュリティセンター中核人材育成プログラム（原則１年間）（H29年度～）【80人/年】	情報処理安全確保支援士（H29年度～）【現在約1.7万人、2020年迄に3万人】 情報セキュリティマネジメント試験(H28年度～)【現在約5.7万人】
		戦略マネジメント層	短期演習（１日間）NISC重要インフラ分野横断演習【２０００人以上】 警察庁　重要インフラ業者等との共同対処訓練【約6100人(H29年中)】		
		実務者層・技術者層	NICT CYDER（1日間/回）（H25年度～）【3000人/年】 NICT サイバーコロッセオ(1~2日間/回)(H28年度～)【2020年迄に220人】	東京電機大Cysec（職業実践力育成プログラム(BP)に認定）（1年間）（H27年度～）【40人/年】	
	ﾍﾞﾝﾀﾞｰ企業のｾｷｭﾘﾃｨ専門職		NICT SecHack365（１年間）（H29年度～）【50人/年】		
高等教育				放送大学※1 放送大学※2 専修学校「職業実践専門課程」制度（２年間）（H25年度～） 高専における人材の育成（警察における講義を含む） enPiT事業による大学（学部）の人材育成拠点整備（H28年度～）【111人/年】 IPA セキュリティキャンプ（22歳以下）における高度人材の発掘（５日間）(H16年度～)【50人/年】	
初等中等教育				情報活用能力（情報セキュリティ含む）の育成の推進	

◆―◆：現在連携中の施策

注：演習、教育、資格・評価基準の分類については、ｻｲﾊﾞｰｾｷｭﾘﾃｨ人材育成総合強化方針（平成28年3月31日ｻｲﾊﾞｰｾｷｭﾘﾃｨ戦略本部決定）に基づくもの。各施策はその中心となる内容に基づいて分類。

各省庁の人材育成関連施策
（平成31年度概算要求関連資料）

警察庁

重要インフラ事業者等と連携した、サイバー攻撃の発生を想定した共同対処訓練

警察では、サイバーテロの標的となる恐れのある重要インフラ事業者等との間で構成するサイバーテロ対策協議会を47都道府県に設置。この枠組み等を通じ、共同対処訓練等を実施し、被害の未然防止と発生時の緊急対処能力の向上に努めている。

【サイバーテロ対策協議会】

【重要インフラ】

情報通信、金融、航空、空港、鉄道、電力、ガス、政府・行政サービス、医療、水道、物流、化学、クレジット、石油

（例）

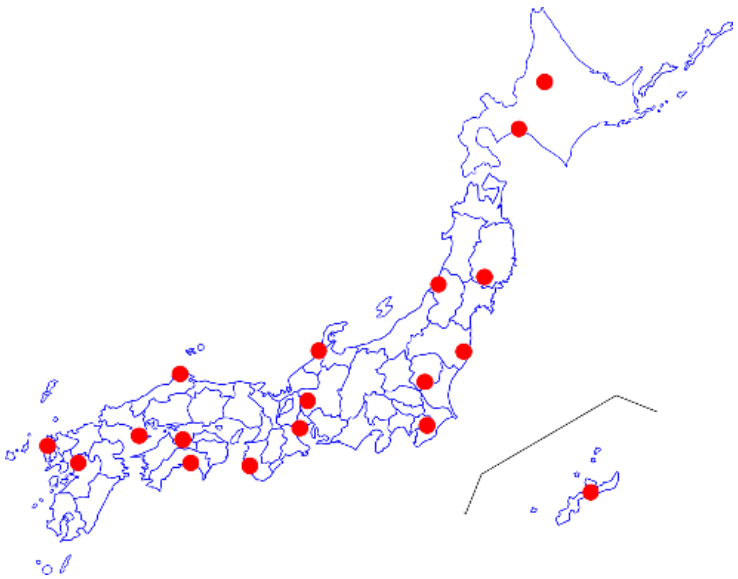
平成29年6月19日、警視庁では、東京都、株式会社東京スタジアム、大会組織委員会等と共同して、東京国際フォーラム及び東京スタジアムにおいて、東京2020オリンピック・パラリンピック競技大会に向けたサイバー攻撃共同対処訓練を実施した。

平成29年8月28日、愛媛県警では、香川県警、四国管区警察局等と連携し、四国電力と共同で、伊方発電所がサイバー攻撃を受けたことを想定した共同対処訓練を実施した。

警察庁

警察における情報技術解析実務を踏まえたサイバーセキュリティ講義

警察庁では、(独)国立高等専門学校機構と連携し、高等専門学校へのサイバーセキュリティ講義を推進。
学生のサイバーセキュリティ分野に対する興味・理解を促進し、人材育成とそれに伴う社会全体の対処能力向上に努めている。



(独)国立高等専門学校機構の情報セキュリティ人材育成プログラムに参加する18の高等専門学校を対象に実施予定。平成30年度は9月6日現在5校実施済。

(例)

平成30年6月27日旭川工業高等専門学校(北海道警察情報通信部情報技術解析課)

学生参加型のデモ実演

捜査支援を模擬した実習

平成30年7月5日岐阜工業高等専門学校(中部管区警察局情報通信部情報技術解析課)

基調講演

デモ実演

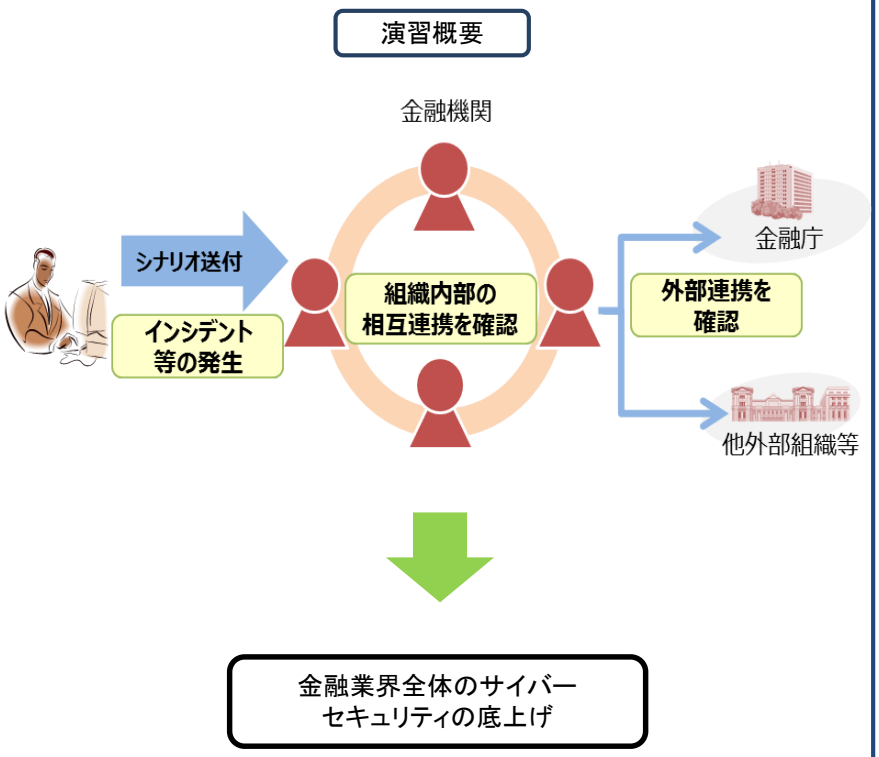
金融分野のサイバーセキュリティ対策強化

平成31年度概算要求：0.6億円
（平成30年度当初予算：0.5億円）

○ 金融業界横断的なサイバーセキュリティ演習の実施

事業概要

- 金融分野におけるサイバー攻撃の高度化が進む中、サイバーセキュリティの確保は、金融システム全体の安定のため喫緊の課題。
- 「金融分野におけるサイバーセキュリティ強化に向けた取組方針」（27年７月公表）に基づき、金融業界全体のインシデント対応能力の更なる向上を図るため、平成30年度、３回目の「金融業界横断的な演習」（Delta Wall Ⅲ）を実施予定。
  （参考）平成30年度演習においては、中小金融機関の底上げを目的に、参加金融機関の対象業態を拡充のうえ、約100先が参加予定（前回は101先）。
- サイバー攻撃へ的確に対応するためには、演習を通じて、現在の対応態勢が十分であるかを確認するなど、PDCAサイクルを回しつつ、対応能力を向上させることが有効。
- 金融分野のサイバーセキュリティ強化には、官民が一体になって取り組んでいくことが重要であり、平成31年度も、引き続き演習を実施予定。
  （注）本演習は、金融庁と参加金融機関の双方で負担（28年度、29年度、30年度）



総務省

実務者層・技術者層 | ベンダー企業のセキュリティ専門職 | 高等教育 | 初等中等教育

セキュリティ人材の育成（ナショナルサイバートレーニングセンター）

平成31年度要求 15.0億円
（30年度予算15.1億円）

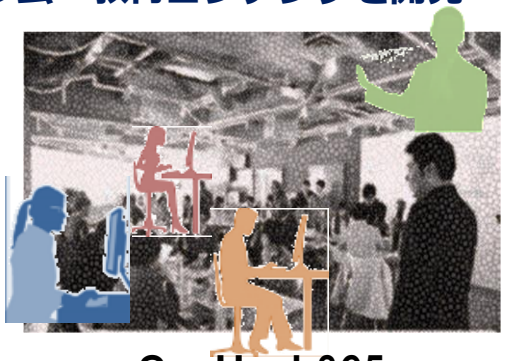
○ 巧妙化・複合化するサイバー攻撃に対し、実践的な対処能力を持つセキュリティ人材を育成するため、平成29年4月より、情報通信研究機構（NICT）の「ナショナルサイバートレーニングセンター」において、以下の実践的サイバー演習等を積極的に推進。

① 国の行政機関、地方公共団体、独立行政法人及び重要インフラ事業者等を対象とした実践的サイバー防御演習 （CYDER）
② 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大会関連組織のセキュリティ担当者等を対象者とした実践的サイバー演習（サイバーコロッセオ）
③ 若手セキュリティイノベーターの育成 （SecHack365）

CYDER

新たな手法のサイバー攻撃にも対応できる演習プログラム・教育コンテンツを開発

サイバーコロッセオ



SecHack365

平成30年度予算 15．1億円

平成31年度要求 15．0億円

実務者層・技術者層

セキュリティ人材の育成（ナショナルサイバートレーニングセンター）①

実践的サイバー防御演習（CYDER）

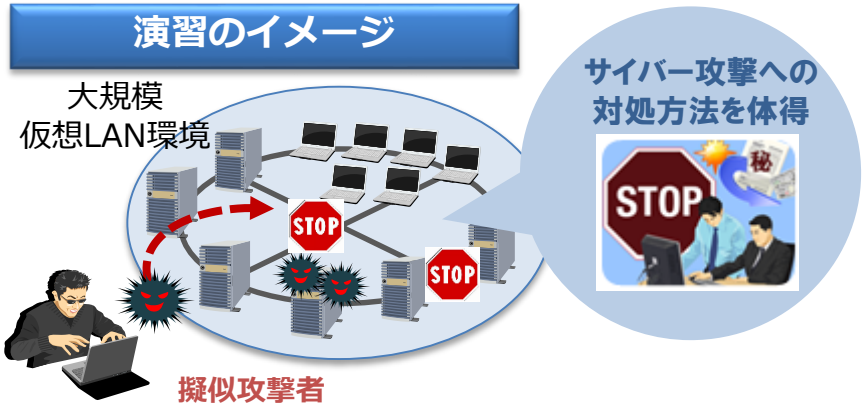
CYDER：CYber Defense Exercise with Recurrence

○ 総務省は、情報通信研究機構（NICT）を通じて、**国の行政機関、地方公共団体、独立行政法人及び重要インフラ事業者等の情報システム担当者等を対象**とした体験型の**実践的なサイバー防御演習（CYDER）**を実施。

○ **受講者は**、組織の情報システム担当職員として、**チーム単位で演習に参加。組織のネットワーク環境を模した大規模仮想LAN環境下で、実機の操作を伴って**サイバー攻撃によるインシデントの検知から対応、報告、 回復までの**一連の対処方法を体験**。

○ 平成29年度については、**全国で100回開催**され、**計3,009名が受講**。

演習のイメージ



CYDER演習風景

■ NICT北陸StarBED技術センターに設置された大規模高性能サーバー群を活用し、行政機関等の実際のネットワークを模した大規模仮想LAN環境を構築。

■ NICTの有する技術的知見を活用し、サイバー攻撃に係る我が国固有の傾向等を徹底分析し、現実のサイバー攻撃事例を再現した最新の演習シナリオを用意。

平成30年度の実施計画

コース	受講対象組織	開催地	開催回数
Aコース（初級）	（全組織共通）	47都道府県	60回
B-1コース（中級）	地方公共団体向け	全国11地域	20回
B-2コース（中級）	国の行政機関等向け	東京	10回
B-3コース（中級）	重要インフラ事業者向け	東京	10回

実務者層・技術者層　ベンダー企業のセキュリティ専門職

セキュリティ人材の育成（ナショナルサイバートレーニングセンター）②－1

東京2020オリンピック・パラリンピック競技大会に向けた実践的サイバー演習（サイバーコロッセオ）

○ 近年さらに高度化・多様化するサイバー攻撃に備え、東京2020オリンピック・パラリンピック競技大会の適切な運営を確保することを目的として、**大会関連組織のセキュリティ担当者等を対象とした、**高度な攻撃に対処可能な人材の育成を行う**実践的サイバー演習「サイバーコロッセオ」を平成30年2月から本格的に実施**。

イメージ図

- 大規模演習環境を用いて、東京大会の公式サイト、大会運営システム等ネットワーク環境を忠実に再現した、仮想のネットワーク環境を構築。
- 仮想のネットワーク環境上で、東京大会時に想定されるサイバー攻撃を擬似的に発生させ、攻撃・防御手法の検証及び訓練を実施。

東京2020オリンピック・パラリンピック競技大会のサイバーセキュリティを確保

実務者層・技術者層 | ベンダー企業のセキュリティ専門職

セキュリティ人材の育成（ナショナルサイバートレーニングセンター） ②－2

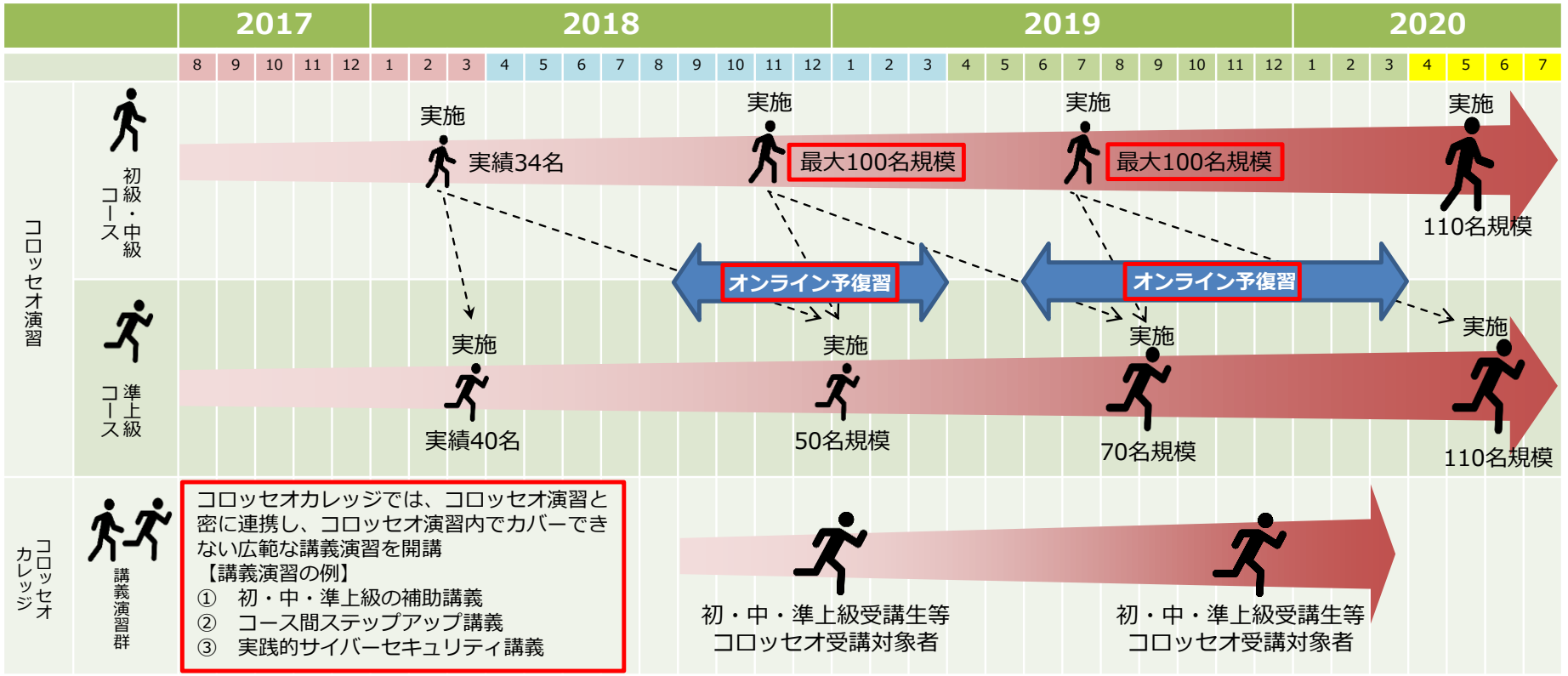
サイバーコロッセオの実施スケジュール

○ 2018年6月、サイバーコロッセオ実施計画を改定し、対象者の受講機会を拡大。

① 初級・中級コースの規模を拡大（2018年度：50名規模（2回）→最大100名規模（3～4回）、2019年度：70名規模（3回）→最大100名規模（3～4回））

② 演習効果をより高めるための講義演習「コロッセオカレッジ」を新設

③ 演習当日以外にも学習可能なオンライン学習コンテンツを提供



※ 目標人数は現時点において公益財団法人東京オリンピック・パラリンピック競技大会組織委員会（以下「組織委」という。）が想定する数字であり、今後、組織委側のニーズを踏まえつつ、必要に応じて見直しを行う予定。

「東京2020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コロッセオ実施計画」（2018年7月24日時点）を基に作成

セキュリティ人材の育成（ナショナルサイバートレーニングセンター） ③

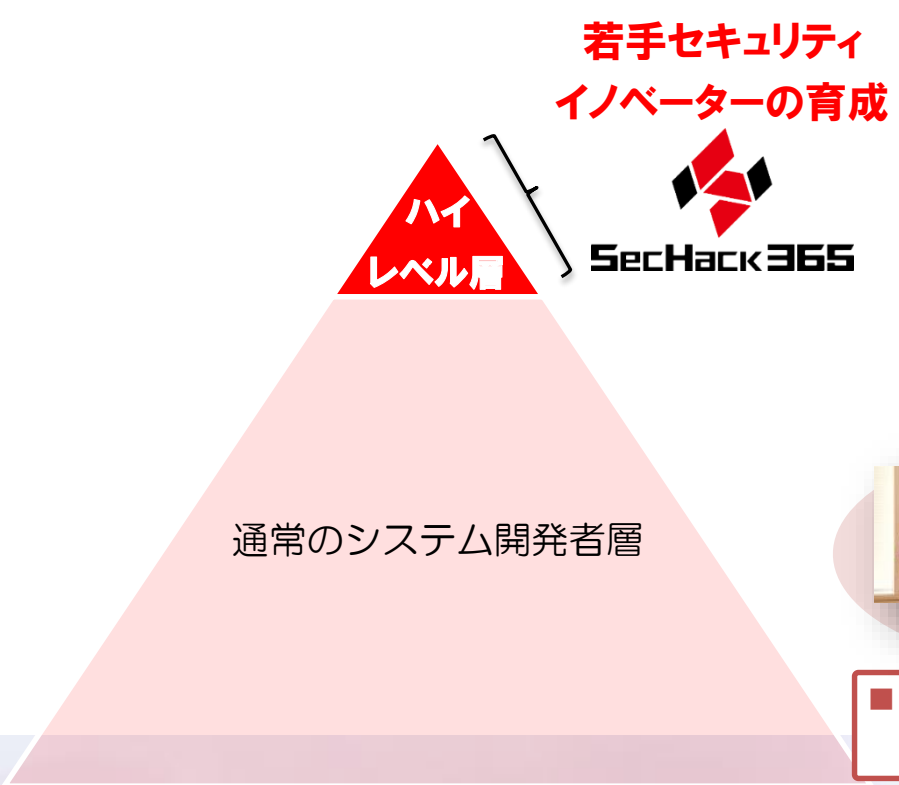
若手セキュリティイノベーターの育成（SecHack365）

セックハックサンロクゴ

○ **未来のサイバーセキュリティ研究者・起業家の創出に向けて**、NICTの持つサイバーセキュリティの研究資産を活用し、**若年層のICT人材を対象に**実際のサイバー攻撃関連データに基づいた**セキュリティ技術の研究・開発を、第一線で活躍する研究者・技術者が１年かけて継続的かつ本格的に指導**。

○ 対象者は、日本国内に居住する**25歳以下の若手ICT人材**（平成29年度は受講者として47名を選定。）

○ 受講者は、NICTの有する遠隔開発環境（NONSTOP（※））を活用し、**年中どこからでも遠隔開発実習を行うことが可能**。また、**集合イベントとして、座学講座（研究倫理）やハッカソン等を実施**。



座学講座

ハッカソン

■ 遠隔開発実習、座学講座、ハッカソン等の組合せによる総合的な人材育成プログラム。

（2）IoTの安心・安全かつ適正な利用環境の構築

・電波を使用するIoT機器が急増し多様化するとともに、それらに対するサイバー攻撃の脅威が増大していることから、下記取組により、国民生活や社会経済活動の安心・安全の確保等を実現

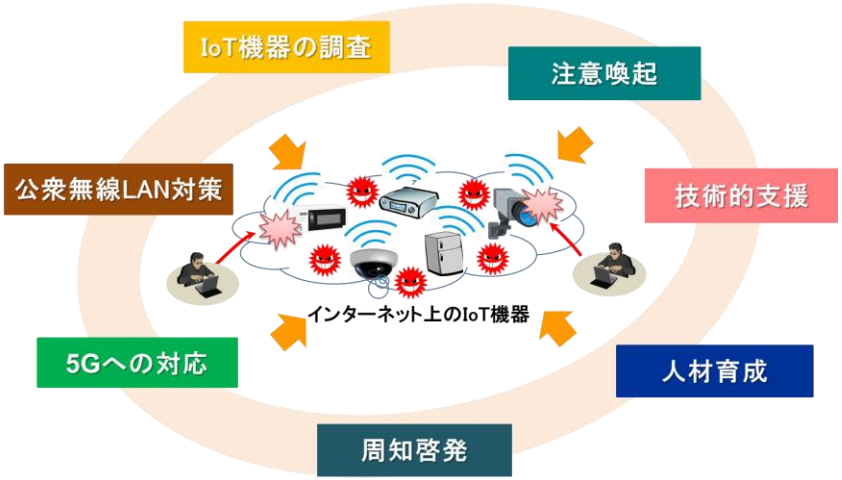
① 改正NICT法に基づきNICTにおいてパスワード設定等に不備のあるIoT機器の調査を実施するとともに、当該機器やマルウェアに感染した機器の利用者への注意喚起にあたり当該利用者からの問合せ対応等を実施

② 地域のIoTセキュリティ人材を育成するための講習を実施するとともに、公衆無線LANのセキュリティ対策に関する周知啓発等を実施

③ ５Ｇ（第５世代移動通信システム）はIoTシステムの基盤技術であるため、５Ｇに係る各レイヤー（IoTデバイス、ネットワーク、クラウド等）におけるセキュリティを総合的かつ継続的に担保する仕組みを整備し、重要インフラ事業者等への周知・啓発を実施

④ 地域の課題解決に資する多様なIoTサービスに係るシステムの適正な運用及び整備等の実証を踏まえてガイドライン等の策定を実施

IoTセキュリティのリテラシー向上



文科省

経営層 | 戦略マネジメント層 | 実務者層・技術者層

平成３１年度概算要求額　32,400千円
（15,150千円）

文部科学省関係機関の情報セキュリティ人材育成　①

《背景・課題》

○「政府機関の情報セキュリティ対策のための統一基準」等の平成28年度改正により、同基準が独立行政法人等にも適用され、政府機関と同水準の情報セキュリティ対策が必要

○一方、大学等については、自主的な情報セキュリティ対策を前提にしつつ、国はその取組が促進するよう、必要な施策等を実施することがサイバーセキュリティ基本法上に規定

○そのような中、大阪大学への標的型攻撃による情報漏えい事案が発生する等、サイバー攻撃の高度化・巧妙化により、標的型攻撃と考えられるセキュリティインシデントが増加

○「サイバーセキュリティ戦略」（平成30年7月閣議決定）においても、大学等の対策が新たに明記され、公・私立を含む大学等に対して、各層別研修及び実践的な訓練・演習の実施について記載

独立行政法人等

統一基準に準拠した体制等の整備や対策の実施
事案対応能力や情報セキュリティに係る知識の向上

大学等（国立大学等に加え、公・私立大学）

自律的かつ組織的な活動能力の向上
マネジメント面・技術面における対策の検討
事案に適切かつ迅速な対処をするための能力の向上

共通的な課題

・日々、高度化・複雑化するサイバー攻撃に対応できる専門知識を持った情報セキュリティ人材が不足

・組織内の役割によって必要となるセキュリティの知識が異なるため、組織として実際に機能する体系的な研修が必要

文部科学省において、関係機関の情報担当者向けに役割に応じた以下の研修を実施

①体系的な各層別セキュリティ研修

②サイバーセキュリティインシデントの対応を行うCSIRT要員を対象としたログ分析等の実践的な演習（10,800千円）

期待できる効果

・体系的な各層別研修により、組織的な活動能力の向上
・各法人の情報セキュリティ水準が向上し、法人が保有している先端技術等の漏えいを防止することで、国際競争力を確保

文部科学省関係機関の情報セキュリティ人材育成 ②

体系的な各層別セキュリティ研修（案）

文部科学省主催の研修において
- ○CISOのガバナンス強化に資するマネジメント研修
- ○現場のセキュリティ対策の状況をCISOに適切に説明できる戦略マネジメント層の育成研修
- ○事案対応や平時の情報セキュセキュリティ対策を行うCSIRT要員への研修
- ○既存の実践的サイバーセキュリティインシデント防御演習の内容を充実
- ○情報セキュリティ監査担当者に対する、監査方法やプロセスに関する研修

以上について、体系的な、実践型のカリキュラムを整備

- CISOマネジメント研修（増要求） 80名程度
- 戦略マネジメント層研修（増要求） 120名程度
- CSIRT要員研修（基礎編）（増要求） 120名程度
- CSIRT要員研修（応用編）（増要求） 120名程度
- 実践的サイバーセキュリティインシデント防御演習
- 情報セキュリティ監査担当者研修（増要求） 120名程度

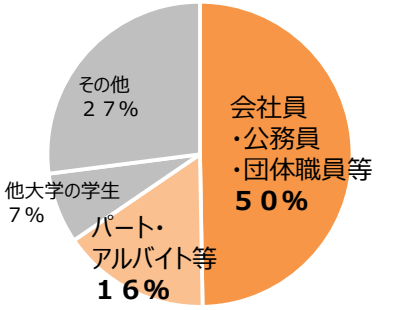
各層別情報セキュリティ研修

放送大学のオンライン教育・連携プログラムの充実

【放送大学の特徴】・社会人を中心とする９万人の幅広い年齢の学生を受け入れ。テレビ・ラジオ・インターネットによる３５０以上の授業科目を開設。
・全国５０の学習拠点において、面接授業（スクーリング）も３千クラス以上開講。

○ 社会人が大学などの教育機関で学びやすくするために必要な取組（上位３項目）
① 学費の負担などに対する経済的な支援（４６．１%）
② **就職や資格取得などに役立つ社会人向けプログラムの拡充**（３５．０%）
③ **土日祝日や夜間における授業の拡充**（３４．０%）
（平成27年度教育・生涯学習に関する世論調査）

○ 放送大学の在学生は、**有職者の学生の占める割合が高い。**



（放送大学の学生構成（平成29年度第2学期））

時間のない社会人向けに、唯一の放送・通信高等教育機関のノウハウを活かし、リカレント・プログラムの供給拡充が必要

放送大学による実践的なプログラムの提供

① **業界団体、学協会等と連携し、実務型科目を大幅拡充。**
（連携例）○ 以下の授業科目を**新たに開講**

データサイエンス、サイバーセキュリティ等

平成３０年度から順次開講
(統計数理研究所、滋賀大学、筑波大学等と協力)

○ 放送大学の**映像授業化ノウハウ**を活かして**実務型研修事業の高度化を支援**

独立行政法人や業界団体等における研修
※現在は、一般社団法人日本内部監査協会等と連携

資格やキャリアアップに関連する授業科目を更に充実

② **蓄積した過去の授業科目を社会人の多様な学習ニーズに合わせ全国へ提供。**
閉講した授業科目のうち学習ニーズの高い番組や各分野の第一人者の名講義等を、新たに開設するＢＳ231チャンネルで放送（本年１０月～）

オンライン科目を１００科目程度へ拡充(４倍増)

他機関のオンラインによる講座の開発・配信への協力

・放送大学におけるリソース（撮影スタジオ、ディレクター、ノウハウ等）の活用や映像配信プラットフォームの提供　等

他大学、学協会、ＭＯＯＣの取組への連携・技術的支援

広く社会へ学習成果を可視化

・産業界と連携した学習証明「エキスパートmini（仮称）」を導入
・小さな科目群として、大学における単位としても活用可能

学習センター（全国50箇所）の活用

・きめ細かな学習・履修相談、ゼミ・勉強会の実施　　・業界団体や学協会等の他機関の利用促進
・他機関と連携した面接授業の実施（他大学との間で数理情報分野に関する調査研究を平成３０年度から開始予定）

文科省

経営層 | 戦略マネジメント層 | 実務者層・技術者層 | ベンダー企業のセキュリティ専門職 | 高等教育

Society5.0に対応した高度技術人材の育成

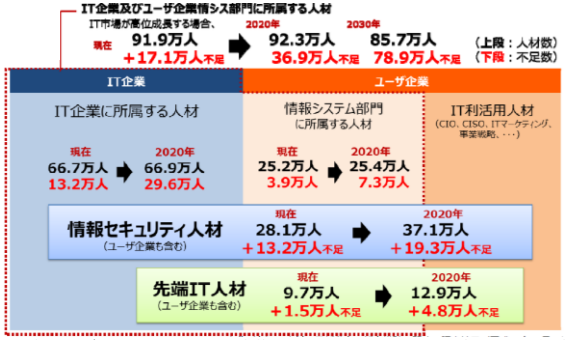
2019年度要求・要望額　1,070百万円
(前年度予算額　1,070百万円)

文部科学省

背景・課題

◆ 第４次産業革命の進展による産業構造の変化に伴い、付加価値を生み出す競争力の源泉が、「モノ」や「カネ」から、「ヒト(人材)」・「データ」である経済システムに移行。

◆ あらゆる産業でＩＴとの組み合わせが進行する中で我が国の国際競争力を強化し、持続的な経済成長を実現させるには、ＩＴを駆使しながら創造性や付加価値を発揮し、日本が持つ強みを更に伸ばす人材の育成が急務。



（資料）IT人材の最新動向と将来推計に関する 調査結果（平成28年6月経済産業省）

事業目的

産学連携による実践的な教育ネットワークを形成し、Society 5.0の実現に向けて人材不足が深刻化しているサイバーセキュリティ人材やデータサイエンティストといった、大学等における産業界のニーズに応じた人材を育成する取組を支援。

取組①　成長分野を支える情報技術人材の育成拠点の形成(enPiT)

産学連携による課題解決型学習(ＰＢＬ)等の実践的な教育の推進により、大学における情報技術人材の育成強化を目指す。

※enPiT（エンピット）：Education Network for Practical Information Technologiesの略

取組①-１　学部学生に対する実践的教育の推進(enPiTⅡ)

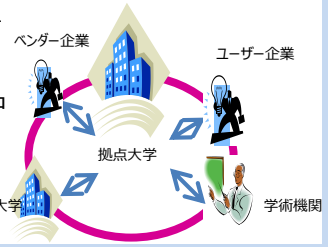
— 事業期間：５年間 財政支援（2016年度～2020年度）
— 運営拠点・単価：1件 × 約45百万円、分野別中核拠点・単価：4件×約108百万円

・「ビッグデータ・AI」「セキュリティ」「組込みシステム」「ビジネスシステムデザイン」の４分野
・大学間連携により、PBL中心の実践的な教育を実施
・教育ネットワークを構築し、開発した教育方法や知見を全国に普及
・産業界と強力な連携体制を構築

取組①-２　IT技術者の学び直しの推進(enPiT-Pro)

— 事業期間：５年間 財政支援（2017年度～2021年度）
— 拠点・単価：5件 × 約66百万円

・大学が有する最新の研究の知見に基づき、情報科学分野を中心とする高度な教育(演習・理論等)を提供
・拠点大学を中心とした産学教育ネットワークを構築し、短期の実践的な学び直しプログラムを開発・実践
・セキュリティ等の特に人材不足が深刻な分野の学び直し推進



取組②　超スマート社会の実現に向けたデータサイエンティスト育成事業

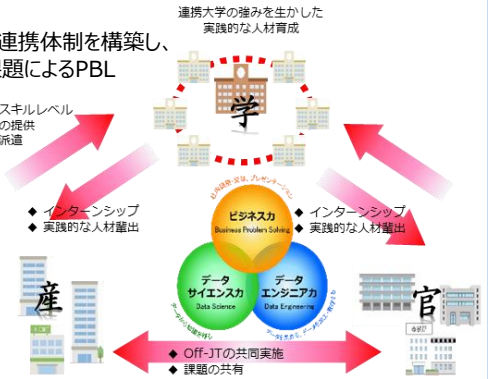
産官学による実践的な教育ネットワークを構築し、文系理系を問わず様々な分野へデータサイエンスの応用展開を図り、それぞれの応用分野で数理・情報的課題解決力を持ち、新しい価値の創造を見いだせる人材(データサイエンティスト)を育成する。

データサイエンティスト育成のための実践的教育の推進

— 事業期間：５年間 財政支援（2018年度～2022年度）
— 拠点・単価：4件 × 約66百万円

・ 産業界や地方公共団体と強力な連携体制を構築し、必要となるビッグデータの提供、実課題によるPBL（共同研究）やインターンシップ等からなる教育プログラムを開発・実践

・ データサイエンスを学ぶ必要に駆られた社会人の学び直しの場を提供し、産官ともに人材不足の中で、Off-JTの産官共同実施の機会やコミュニティ形成を醸成



文科省

実務者層・技術者層

「職業実践力育成プログラム」（ＢＰ）認定制度

－ Brush up Program for professional －

Brush up Program for professional

○　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「職業実践力育成プログラム」（ＢＰ）として文部科学大臣が認定。（平成30年４月現在、222課程を認定）

【目的】①地方創生、②女性活躍、③中小企業活性化、④非正規労働者のキャリアアップ等に資す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

【認定要件】

○ 大学、大学院、短期大学及び高等専門学校の**正規課程及び履修証明プログラム**

○ **対象とする職業の種類及び修得可能な能力を具体的かつ明確に設定し、公表**

○ 対象とする職業に必要な実務に関する知識、技術及び技能を修得できる教育課程

○ 総授業時数の一定以上（５割以上を目安）を以下の２つ以上の教育方法による授業で占めている

①実務家教員や実務家による授業 （専攻分野における概ね５年以上の実務経験）	**②双方向若しくは多方向に行われる討論** （課題発見・解決型学修、ワークショップ等）
③実地での体験活動 （インターンシップ、留学や現地調査等）	**④企業等と連携した授業** （企業等とのフィールドワーク等）

○ 受講者の成績評価を実施　○ 自己点検・評価を実施し、結果を公表（修了者の就職状況や修得した能力等）

○ **教育課程の編成及び自己点検・評価において、組織的に関連分野の企業等の意見を取り入れる仕組みを構築**

○ **社会人が受講しやすい工夫**の整備（週末・夜間開講、集中開講、ＩＴ活用等）

認定により、

①社会人の学び直す選択肢の可視化、

②大学等におけるプログラムの魅力向上、

③企業等の理解増進

を図り、厚生労働省の教育訓練給付制度とも連携し、社会人の学び直しを推進

○東京電機大学　Cysec「国際化サイバーセキュリティ学特別コース」

【概要・目的】　ICTシステム管理者・開発者やサイバーセキュリティ技術者等を対象に、サイバーセキュリティの技術だけでなく、法律や倫理等の関連する分野の教育を行い、高度な専門家を養成。

【プログラムの特徴】　サイバーセキュリティに関する法・倫理、インシデント対応、サイバーディフェンス等の科目で構成され、関連企業の実務家による授業、グループワークや実践演習などを実施。

【受講期間】　1年

【社会人の受講しやすい工夫】　夜間・週末開講、長期履修可

専門学校における職業教育の充実
「職業実践専門課程」の文部科学大臣認定制度

平成23年1月　中央教育審議会「今後の学校におけるキャリア教育・職業教育の在り方について」答申

○　職業教育を通じて、自立した職業人を育成し、社会・職業へ円滑に移行させること、また、学生・生徒の多様な職業教育ニーズや様々な職業・業種の人材需要にこたえていくことが求められており、このような職業教育の重要性を踏まえた高等教育を展開していくことが必要。
○　高等教育における職業教育を充実させるための方策の一つとして、職業実践的な教育のための新たな枠組みを整備。
⇒　新たな学校種の制度を創設するという方策とともに、既存の高等教育機関において新たな枠組みの趣旨をいかしていく方策も検討。

平成25年7月 「専修学校の質保証・向上に関する調査研究協力者会議」報告

「新たな枠組み」の趣旨を専修学校の専門課程においていかしていく先導的試行として、企業等との密接な連携により、最新の実務の知識等を身につけられるよう教育課程を編成し、より実践的な職業教育の質の確保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。

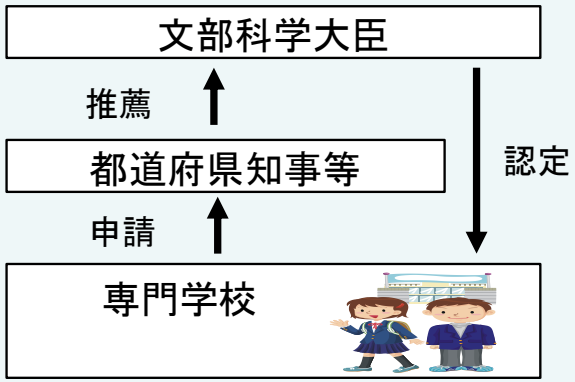
⇒平成25年8月　「専修学校の専門課程における職業実践専門課程の認定に関する規程(文部科学省告示第133号)」を公布・施行

⇒平成26年3月31日　「職業実践専門課程」を文部科学大臣が認定し、官報で告示。 4月から認定された学科がスタート

平成29年3月　これからの専修学校教育の振興のあり方について（報告）

職業実践専門課程は、**教育の高度化と改革を目指す専門学校の取組の枠組**として位置づける。

認定要件等



－認 定 要 件－

企業等との「組織的連携」　取組の「見える化」

○　修業年限が2年以上
○　企業等と連携体制を確保して、授業科目等の教育課程を編成
○　企業等と連携して、演習・実習等を実施
○　総授業時数が1700時間以上または総単位数が62単位以上
○　企業等と連携して、教員に対し、実務に関する研修を組織的に実施
○　企業等と連携して、学校関係者評価と情報公開を実施

文科省

高等教育

情報セキュリティ人材の育成

2019年度要求・要望額　408百万円
(前年度予算額　398百万円)

背景

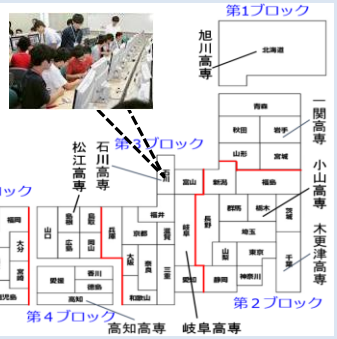
○Society5.0時代を迎えるに当たって、これまでのIT技術教育を基盤に、ビッグデータやIoT、人工知能（AI）を使いこなせる**先端IT人材の育成が急務**となっている。
○また、あらゆるものがインターネットに接続され、ITを活用したサービスが拡大する中、**あらかじめセキュリティを考慮したセキュリティ・バイ・デザインができる人材**の育成が必要である。
○これらを実現するため、**産学官協働による需要（企業等）と供給（教育機関）の好循環（サイバーセキュリティエコシステム）の形成**が必要である。

これまで

<第１フェーズ>
○2016度に整備した**先行５拠点**（一関、木更津、石川、高知、佐世保）において、「情報セキュリティ人材」の育成に必要な**教育を実践・検証**し、理想的な**環境整備と実効性のある教育方法を確立**。

<第２フェーズ>
○**後発５拠点**（旭川、小山、岐阜、松江、熊本）の**環境整備を実施**し、**全国10ヶ所で「情報セキュリティ人材」の発掘・育成を実施**。
○情報セキュリティに係る教育プログラムや、専門学科毎のケーススタディを学ぶ**分野別教材を開発**。全高専へ展開。

全国の高等専門学校生が共同で利用できるサイバーレンジ（実践的な演習環境）を整備



事業内容

<第3フェーズ>
これまでの取組を継続するとともに、日々進化するサイバーセキュリティ技術に対応するため、
①**情報セキュリティ教育の徹底**（効果的なモラル・リテラシー教育の事例共有、情報系以外の分野におけるセキュリティマインドの理解等）
②IPA等の**外部機関との連携により**、セキュリティ教育を実践できる**教員の高度化を図り、セキュリティ教育にフィードバック**。
③日々進化するサイバーセキュリティ技術の高度化に対応するため、**演習拠点環境を更新**（2拠点）。

	2016	2017	2018	2019	2020	2021
拠点整備	5拠点	5拠点				
環境更新（ソフトウェア中心）			3拠点	2拠点	3拠点	2拠点

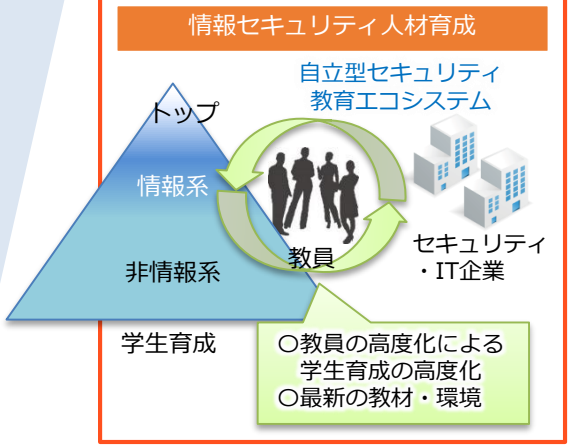
【拠点整備・環境更新の年次計画イメージ】
◎ 拠点整備 ⇒ 2016年度、2017年度の2カ年で整備
◎ 環境更新 ⇒ 2018年度から４年周期で更新
※日々進化しているサイバー攻撃技術にも対応するため、定期的な環境更新（アップデート）が必要。

目標とする姿

○**情報セキュリティインシデントに対応できる技術者の早期育成**。（トップ・情報系）

○各専門分野において「守るべきものは何か？」を知った**セキュリティスキルを持った高専生を継続的に育成（約1万人/年）**。（情報系・非情報系）

○企業等と連携し情報セキュリティ人材育成エコシステムの構築。



次世代の教育情報化推進事業

２０１９年度要求・要望額 １２８百万円
（前年度予算額 １０８百万円）

趣旨

全国の小・中・高等学校において新学習指導要領の趣旨を踏まえ、全ての学習の基盤となる「情報活用能力」の育成に取り組めるよう、優れた指導事例の創出・普及や教員研修用教材の開発等の支援策を講じる。
とりわけ、新たに必修化された小学校におけるプログラミング教育の推進に重点的に取り組む。

新学習指導要領

（小学校学習指導要領、中学校学習指導要領　平成29年3月31日公示、高等学校学習指導要領　平成30年3月30日公示）

- 「情報活用能力」を「学習の基盤となる資質・能力」と位置付け、「教科横断的な視点から教育課程の編成を図」り、育成していく
- 「コンピュータや情報通信ネットワークなどの情報手段を適切に活用した学習活動の充実を図る」
- 小学校においては、「児童がプログラミングを体験しながら、コンピュータに意図した処理を行わせるために必要な論理的思考力を身に付けるための学習活動」を、「各教科等の特質に応じて」、「計画的に実施する」
- 高等学校情報科については、共通必履修科目「情報Ⅰ」を新設し、全ての生徒が、プログラミング、ネットワーク（情報セキュリティを含む）やデータベースの基礎等について学ぶよう改訂・充実する。
- 発展的な内容の「情報Ⅱ」を新設し、データサイエンスや情報システムの設計等について取り扱う

小学校　2020年度から全面実施
中学校　2021年度から全面実施
高等学校　2022年度から学年進行で実施

○新学習指導要領の趣旨の実現に向けた情報教育及びICT活用の推進に関する調査研究

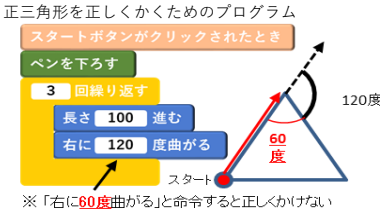
新学習指導要領の趣旨の実現に向けて、推進校における実践研究を通じた優れた事例及びモデルの創出を目指す

① 情報活用能力を育む教科横断的で体系的なカリキュラム・マネジメント事例（GP）の創出
② 「主体的・対話的で深い学び」（アクティブ・ラーニング）を実現するICTを効果的に活用した指導事例（GP）の創出

○小学校プログラミング教育支援推進事業

小学校プログラミング教育の円滑な実施に向けて、指導事例の創出・普及や研修充実のための教材開発等を実施

① 全国の小学校において参考となる、新学習指導要領の趣旨を踏まえたプログラミング教育の指導事例（GP）の創出と普及
② 各小学校の校内研修において活用できる教員研修用教材（映像教材やeラーニング教材）を発展・充実
③ 地域の研修リーダーとなる教員等を対象としたセミナーの実施



未来投資戦略2018【抜粋】
（平成30年6月15日閣議決定）

・平成32年度から全ての小学校でプログラミング教育を効果的に実施するために、来年度から教員が教材や指導方法等に習熟できるよう、未来の学びコンソーシアムの活動等により、全国の教育委員会や学校、企業等と協働して、ポータルサイト等を活用しながら教材開発や教員研修の質の向上を実現する。
・AI活用のための基礎的な素養を身に付けさせるため（略）、学習指導要領の改訂を全国の学校現場で着実に実現する。このため、eラーニング等による効果的な教員の研修や教材の充実、外部人材の活用等に取り組む。

「未来の学びコンソーシアム」と連携
・創出された指導事例等を全国の小学校への情報提供（コンソーシアムのポータルサイトを通じて発信）

○新学習指導要領に対応した高等学校情報科担当教員の指導力向上

情報科担当教員を対象とした都道府県等の研修でも活用できる教員研修用教材の作成・配布

データサイエンス、プログラミング、サイバーセキュリティなどの最新の情報技術の知識や、新学習指導要領に対応した指導方法等に関する研修について、各都道府県教育委員会等の計画的な実施を支援

情報モラル教育推進事業

２０１９年度要求・要望額　63百万円
（前年度予算額　20百万円）

趣 旨

携帯電話・スマートフォンやSNSが子供たちにも急速に普及する中で、児童生徒が、自他の権利を尊重し情報社会での行動に責任を持つとともに、犯罪被害を含む危険を回避し、情報を正しく安全に利用できるようにするため、学校おける情報モラル教育は極めて重要である。
指導資料の改善・充実や児童生徒向け啓発資料の作成・配布等により、学校段階、児童生徒の発達段階等に応じて、情報モラル教育の着実な実施を図る。

【子供たちを取り巻く状況】

- 高校生の95.9%、中学生の58.1%、小学生（満10歳以上）の29.9%がスマートフォンを所有
  高校生の74.2%、中学生の56.7%、小学生の33.4%がインターネットを１日（平日）に２時間以上利用
  （内閣府「平成29年度青少年のインターネット利用環境実態調査」）
- SNS等で被害にあった子供の数は増加傾向が継続し、平成29年度に1,813人で過去最多
  （警察庁「平成29年度におけるSNS等に起因する被害児童の現状と対策について」）
- 若年層が不正アクセス等の加害者となる事案も発生

【学習指導要領の改訂】

- 新学習指導要領においても従前に引き続き情報モラルの育成を重視
- 学習指導要領解説においては、インターネット利用に伴う犯罪被害の防止の必要性や、児童生徒の発達の段階に応じて情報や情報技術の特性についての理解に基づく情報モラルを身に付けさせることを強調

【SNS等に起因する犯罪被害の防止】

- 座間市における事件をふまえ、学校教育では「情報モラル教育に関する教師用指導資料を改訂し配布するとともに、児童生徒向け啓発資料を作成するなど、学校における情報モラル教育の充実を図る。」
  （「座間市における事件の再発防止策について」 平成29年12月19日
  座間市における事件の再発防止に関する関係閣僚会議【抜粋】）

１．情報モラル教育の推進に係る指導資料の改善〈委託〉24百万円

平成27年度に作成した指導資料（動画教材を含む。）について、インターネットやスマートフォン利用者の低年齢化、最新のトラブルや被害の状況等を踏まえて、内容の改善・充実を図る。

主な改善点

- 低年齢層(小１～４年生)に対応した指導資料や動画教材を作成
- 実践校の調査研究をもとにモデル指導案等を作成
- ネット依存・ネット被害やSNS等におけるトラブルに係る内容の充実、その他最新の状況・動向の反映

２．児童生徒向け啓発資料の作成・配布〈委託〉30百万円

携帯電話・スマートフォンやSNSを適切に利用できるようにするため、児童生徒向け啓発資料を作成・配布する。

３．情報モラル教育指導者セミナーの開催〈委託〉9百万円

学校における今日的課題を踏まえた情報モラル教育の取組の推進に資するため、教員等を対象とした実践等を含めたセミナーを実施する。

経産省

経営層 | 戦略マネジメント層 | 実務者層・技術者層 | ベンダー企業のセキュリティ専門職

産業系サイバーセキュリティ推進事業

平成31年度概算要求額 20.1億円
（19.1億円）

事業の内容

事業目的・概要

- 近年、企業や個人の情報を狙ったサイバー攻撃にとどまらず、プラントやインフラそのものの停止を狙い、制御システムまで含めた社会システム全体を標的とするサイバー攻撃のリスクが高まっています。（※制御システム：工場やプラントの機械や設備などのコントロールを行うために用いられるシステムのこと）
- 国家として、安全・安心な社会を築くためには、重要インフラや我が国経済・社会の基盤を支える産業における、サイバー攻撃に対する防護力を強化することが必須です。
- そのため、（独）情報処理推進機構（IPA）に29年4月に設立した「産業サイバーセキュリティセンター（Industrial Cyber Security Center of Excellence）」において、模擬プラントを用いた演習を通じて、官民の共同によりサイバーセキュリティ対策の中核となる人材を育成します。また、実際の制御システム等の安全性検証等により、産業のサイバーセキュリティ対策のノウハウを創出します。

成果目標

- 模擬プラント等を活用し、重要インフラ事業者等において、サイバーセキュリティの総合的な戦略立案を担う人材を毎年100人程度育成します。
- 本事業で安全性検証等を行った分野における主要企業において、継続的または新規のサイバーセキュリティ対策を講じることを目指します。

条件（対象者、対象行為、補助率等）

国 → 交付金 → （独）情報処理推進機構

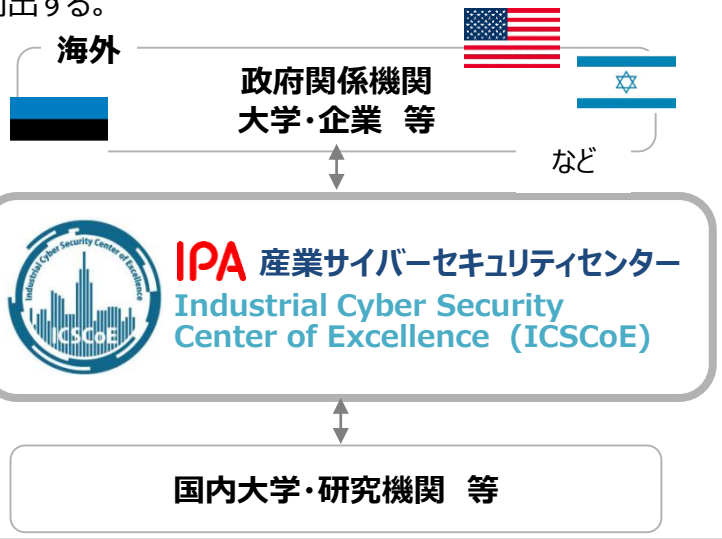
事業イメージ

模擬プラントを用いた演習等を通じた人材育成

- 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。専門家と共に安全性・信頼性の検証や早期復旧の演習を行う。
- 最新の攻撃情報の調査・分析結果に応じてプログラムのアップデート等を実施。
- 海外との連携も積極的に実施。

実際のシステムの安全性・信頼性検証等

- 社会インフラ等で活用されている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ことで、業界全体で活用可能なサイバーセキュリティ対策のノウハウを創出する。



戦略 マネジメント層 | 実務者層・技術者層 | ベンダー企業のセキュリティ専門職

産業系サイバーセキュリティ推進事業 ①

IPA産業サイバーセキュリティセンター 中核人材育成プログラム（１年コース）

- 世界的にも限られている、制御系セキュリティにも精通する講師を招き、テクノロジー、マネジメント、ビジネス分野を総合的に学ぶ1年程度のトレーニングを実施。

制御系セキュリティにも精通する講師陣

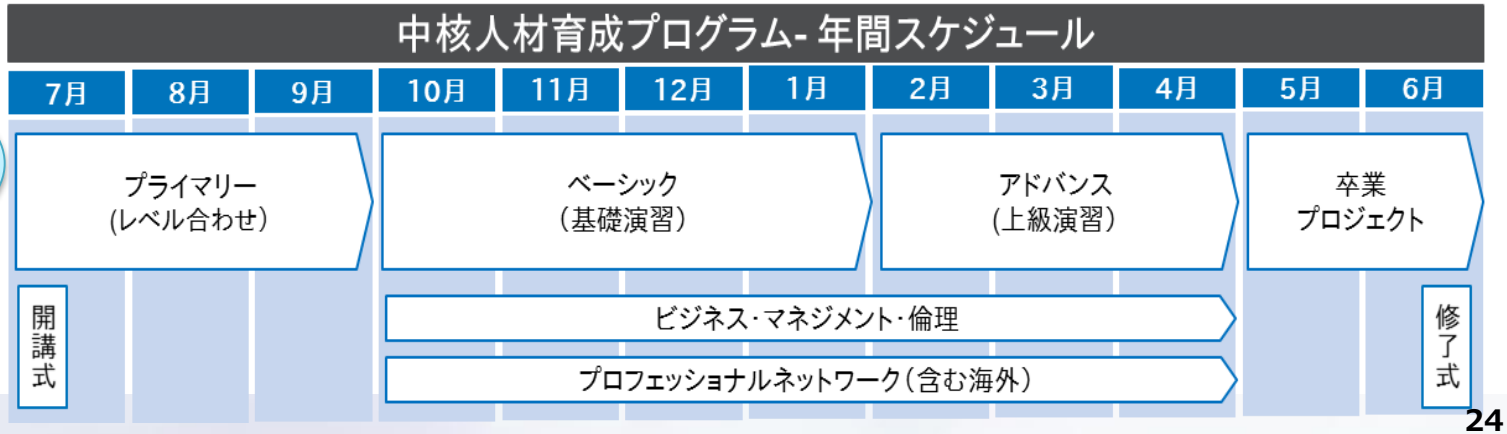
門林 雄基
奈良先端科学技術大学院大学
情報科学研究科 教授

小林 和真
制御**システム**
セキュリティセンター
顧問

満永 拓邦
東京大学
情報学環　特任准教授

越島 一郎
名古屋工業大学大学院
工学研究科　教授

１年を通じた集中トレーニング



産業系サイバーセキュリティ推進事業 ②

IPA産業サイバーセキュリティセンター 責任者向けプログラム（短期・中期）

- 最高情報セキュリティ責任者（CISO）や戦略マネジメント機能を担う人材に必要なセキュリティ対策に関するトレーニングを行う短期・中期プログラム。

【業界別トレーニング（2日間）】

- 産業基盤系業界（金属、石油、化学等）に係る制御システムユーザー企業、ハード・ソフトウエアベンダー企業等のCISOや責任者等を対象に業界別に企業が直面するサイバーリスクへの対応について講義を実施。
- 仮想企業を想定した、複数の具体的なシナリオ形式による実践的演習を実施。

【国際トレーニング（2日間）】

- 日本における社会インフラ、産業基盤の制御システムを有する企業の部長、CISO、CIO等を対象に、企業を守るために必要なスキルとメソッドを提供するプログラム。
- 参加者と海外セキュリティ専門家間のコミュニティやリレーションの構築も目的とする。

【戦略マネジメント系セミナー（全7回）】

- 現在CISOやその補佐を務めている方や、戦略企画層の方を対象にサイバーセキュリティのリスク管理や、インシデント対応等のプログラムを、2か月間集中して実施。
- 講義・演習・ケースディスカッションを通じてセキュリティマネジメントについてトレーニングを実施。

経産省

J-Startup

独立行政法人情報処理推進機構（IPA）運営費交付金

平成31年度概算要求額 56.0億円
（49.0億円）

事業の内容

事業目的・概要

- 独立行政法人情報処理推進機構（IPA）が行う業務に必要な運営費を交付し、以下の事業を行います。

（１）情報セキュリティ対策の強化
重要インフラのみならず、中小企業及び国民にまでセキュリティの大切さの認識を高め、サイバー攻撃被害の未然防止やセキュリティ対策に係るガイドラインの普及促進等、セキュリティの強化を図ります。

（２）ＩＴ人材育成の強化
ICTに関する基礎的なスキルをあらゆる人材が身につけるとともに、社会イノベーションを牽引する高度な人材を育成します。

（３）調査・分析・情報発信機能の強化
常に最先端の技術動向をおさえ、社会実装に役立つ情報を発信し、社会イノベーションの基盤となります。

（４）デジタルトランスフォーメーション（DX）の促進
情報資産の「見える化」指標策定や診断スキームの構築等により企業のDXを促進します。

成果目標

- 重要インフラ企業が取組む新規・追加のセキュリティ対策を第四期中期目標期間中に500社以上にします。
- ＩＴ人材の発掘・育成の成果として、未踏事業修了生による新たな社会価値創出を第四期中期目標期間中に50件以上にします。

条件（対象者、対象行為、補助率等）

国 → 交付金 → 情報処理推進機構（IPA）

事業イメージ

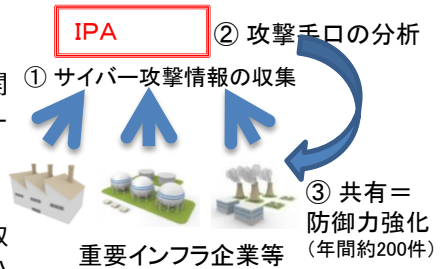
（１）情報セキュリティ対策の強化

- サイバー攻撃に関する情報収集、対処方法の提示

重要インフラ等におけるサイバー攻撃に関する情報収集・情報共有のほか、サイバー攻撃に対する注意喚起を発出します。

- セキュリティアクション制度の普及

中小企業自らが情報セキュリティ対策に取り組むことを宣言する制度に参画する中小企業数を加速度的に増やします。



（２）ＩＴ人材育成の強化

J-Startup

- 未踏IT人材発掘・育成事業の実施及び拡充

突出した才能を持つITクリエータや、産業界を牽引・リードするIT等のトップ人材を発掘・育成します。
また、将来的に有望と見込まれる分野として特定した新たな技術領域を主導する先端IT人材を創出するため、新たな人材育成プログラムを創設いたします。
J-Startup企業に対して、成果報告会等のイベントへ優先的に招待し、ITトップ人材とのマッチングを促進します。


（未踏IT人材発掘・育成事業）

（３）調査・分析・情報発信機能の強化、（４）DXの促進

- IoT、AIをはじめ、最先端のICTに関する技術動向の調査・分析、新しい技術の指針・ガイドラインを整備し、国民・企業の役に立つ形で情報を発信します。
- DX推進における課題を解決するため、情報資産の「見える化」指標の策定や診断スキームの構築、システム構築に最適な契約の在り方や共通プラットフォームの構築に向けた検討を行い、企業のDXを促進します。

独立行政法人情報処理推進機構（IPA）運営費交付金

セキュリティ・キャンプ

- 複雑かつ高度化してい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(22歳以下)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**。これまでの**セキュリティ・キャンプ全国大会(2004年より開始,計15回開催)**については累計で**748名**が受講。
- 更に、地方における**セキュリティ・キャンプ地方大会**(2013年より開始)も併せて実施することにより、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

清水郁実さん
2015年修了（当時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、３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。

経産省

戦略マネジメント層 | 実務者層・技術者層 | ベンダー企業のセキュリティ専門職

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。2020年までに登録者3万人超を目指す。
- 平成30年10月1日時点での登録人数は17,360名。

◆ 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。**

◆ 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。**

米国大統領令に基づくサイバーセキュリティ人材育成に関する報告書（2018年5月）

2017年５月の「連邦政府ネットワーク及び重要インフラのサイバーセキュリティ強化に関する大統領令」に基づき、**2018年5月**、**NIST**（国立標準技術研究所）が米国における**官民のサイバーセキュリティ人材の育成強化に関する報告書を策定・ 公表**。

概要

(1) 現状

○ 米国内では**約30万人のサイバーセキュリティ人材の求人**（2017年8月現在）。また、グローバルには、2022年には約180万人の不足が発生するとの試算もあり。

○ **初級者的レベルから高度な知識・技能を必要とするレベルまで幅広い人材**が求められており、**人材獲得の競争**も激しくなっている。

○ 経営層は、**サイバーセキュリティに関する能力・資格のみならず、事業分野に関する知識・スキルを有する人材**を求めている。

(2) 主な課題

○ 米国は、サイバーセキュリティ人材の育成に関する、速やか、かつ、持続的な取組を推進することが重要。

○ 具体的には、**経営層のニーズに合致する人材を育成・確保するための教育プログラムの提供**、**社会人等の学び直し**、**初等中等教育の充実**、**求人や教育・研修プログラムに関する包括的かつ信頼性の高いデータ提供**等を推進することが必要。

(3) 今後、推進すべき取組

- 安全保障及び経済的発展に資する人材の育成・強化に係るビジョン及びアクションプラン、官民連携のための「行動規範（Call for Action）」の策定
- 高品質かつ効果的な教育プログラム等を提供するための予算の確保
- 政府機関におけるサイバーセキュリティ人材の採用・育成・確保に関する取組の推進
- 学び直しの推進（例：ハンズオン演習、オンライン学習、教員・講師の確保、必要な予算の確保）
- 官民連携の下、経営層のニーズに合致する人材の育成・強化の推進（例：NICEフレームワークの活用、キャリアパスやカリキュラムのモデル化、州ごとに一つ以上の連合（alliance）の整備、人材育成に関する情報ハブ（clearing house）の整備）
- 人材育成への投資効果を定量的に把握するための手法の開発・活用