NISC National center of Incident readiness and Strategy for Cybersecurity

資料１-１

サイバーセキュリティ人材育成における施策間連携について

平成２９年９月

内閣官房　内閣サイバーセキュリティセンター

本WGの主な検討事項

各層の人材像と求められる知識・スキルを明確化し、各層別のカリキュラムの方向性を提示するとともに、各施策間の連携を図る。

- 企業において育成すべき**各層（経営層、戦略マネジメント機能、システム担当、システム構築・運用担当）別の人材像やキャリアパスの明確化**
  - 特に、各部門におけるセキュリティを含めた**戦略マネジメント機能**を担う人材
  - 高度人材の定義、位置付けの整理

- セキュリティ人材育成の前提となる**ITの基本的知識**を明らかにするとともに、それを踏まえた**各層別のカリキュラム（短期・中長期）の方向性を提示**

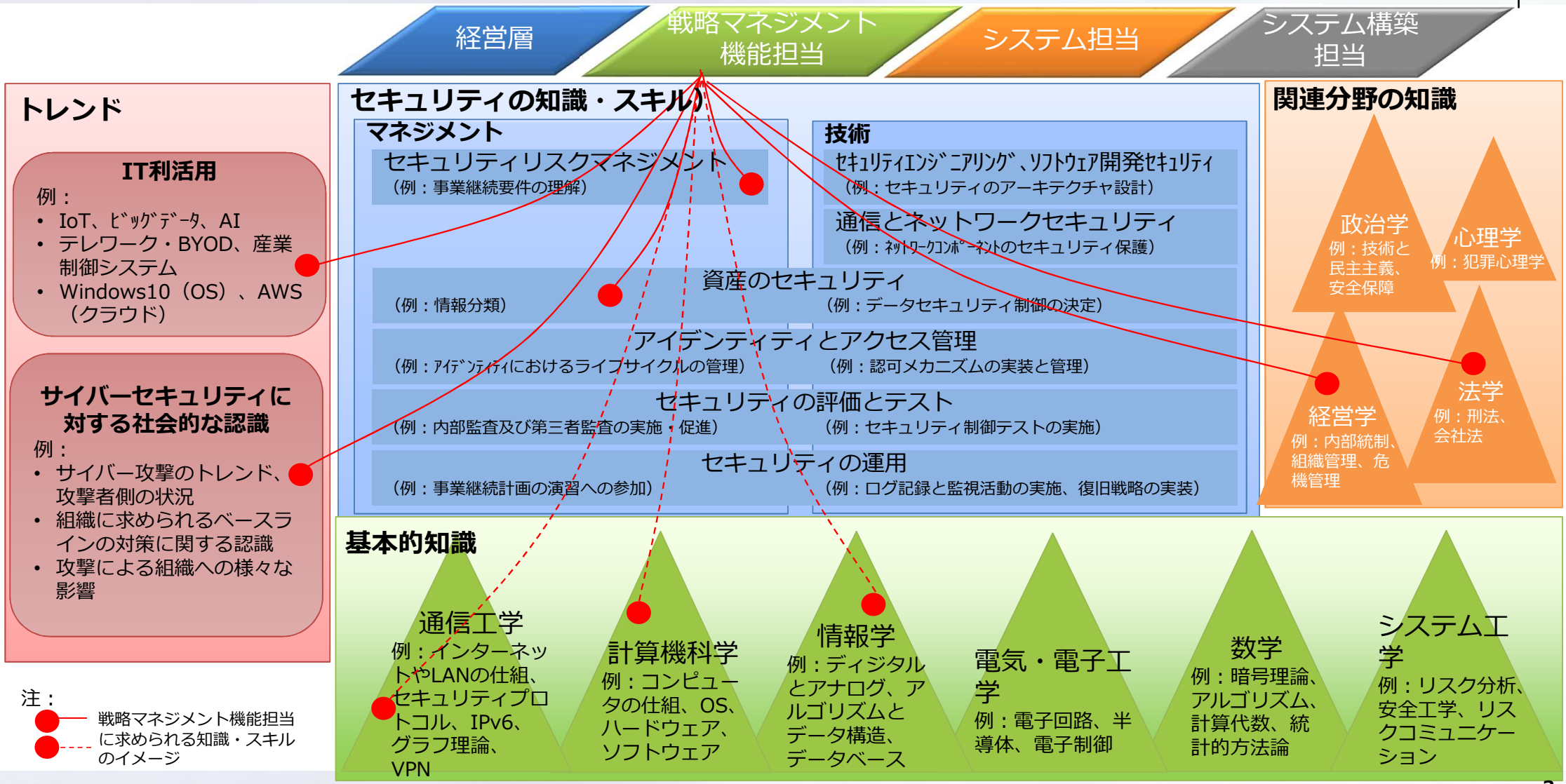
- 各層別のカリキュラムを意識した**各省の人材育成施策に関する全体像を整理し、連携策の検討**を推進

- カリキュラムに基づく**教材について、R&D**を推進

- 人材育成・確保に向けた**産学官連携の在り方・具体的方策**の明確化

→上記の内容を踏まえ、今後の取組の方向性については、**次期「サイバーセキュリティ戦略」**に反映していく。

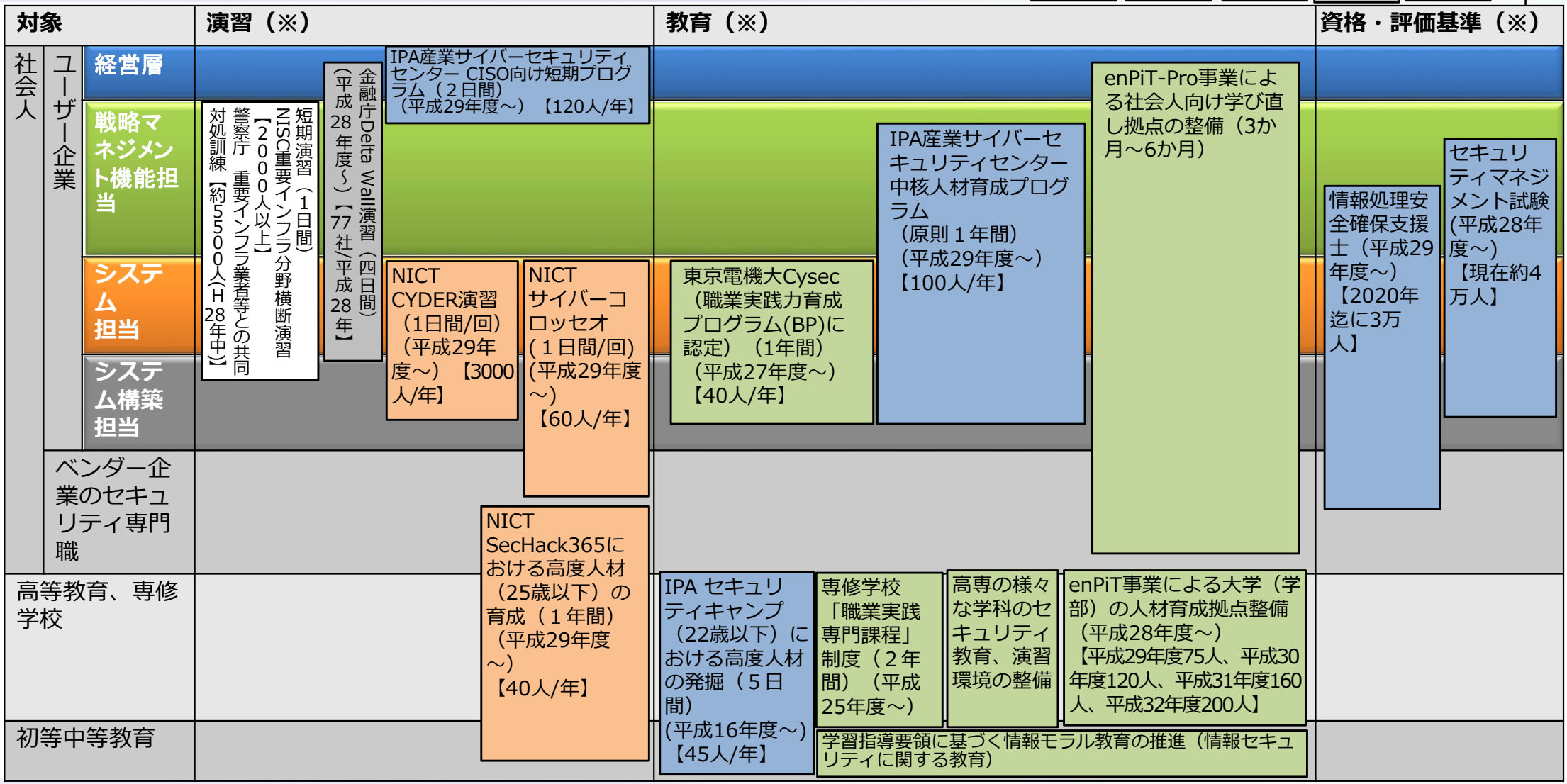
カリキュラムの考え方（イメージ）



注：
戦略マネジメント機能担当に求められる知識・スキルのイメージ

各省の人材育成施策に関する全体像（イメージ）

総務省　文科省　経産省　金融庁　その他



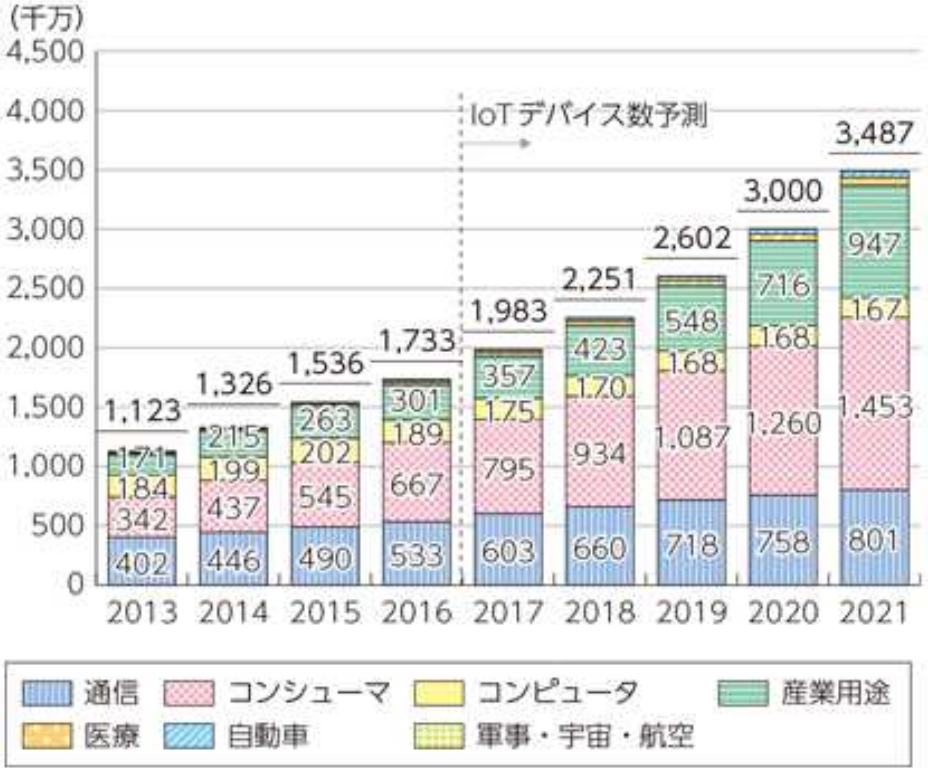
※演習、教育、資格・評価基準の分類については、サイバーセキュリティ人材育成総合強化方針（平成28年3月31日サイバーセキュリティ戦略本部決定）に基づくもの。各施策は、その中心となる内容に基づいて分類。

空白ページ

参考資料

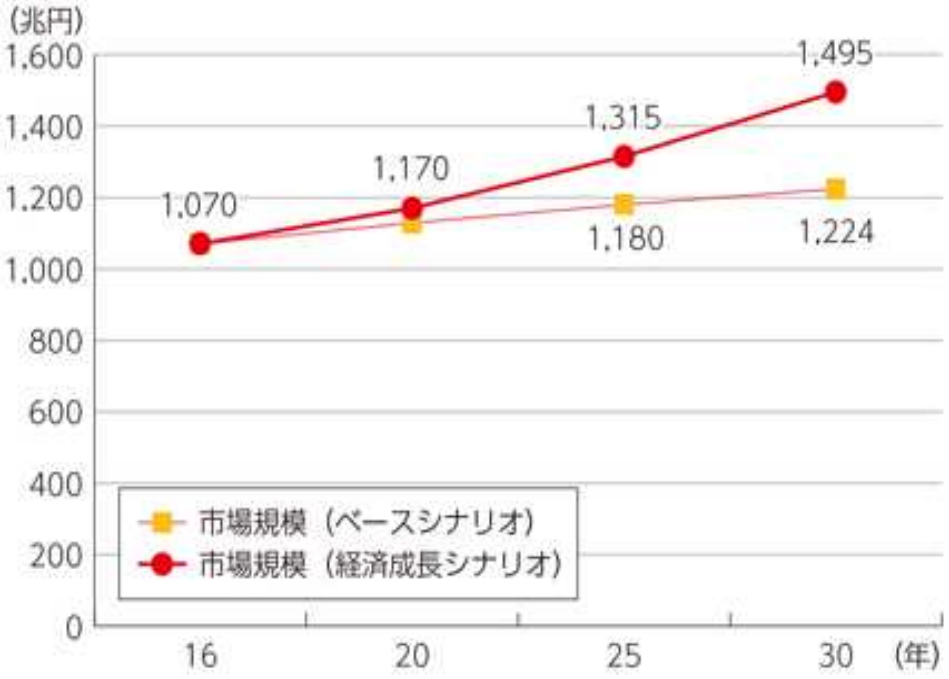
IoTをはじめとしたビジネスにおけるIT利活用の広がり

世界のIoTデバイス数の推移及び予測



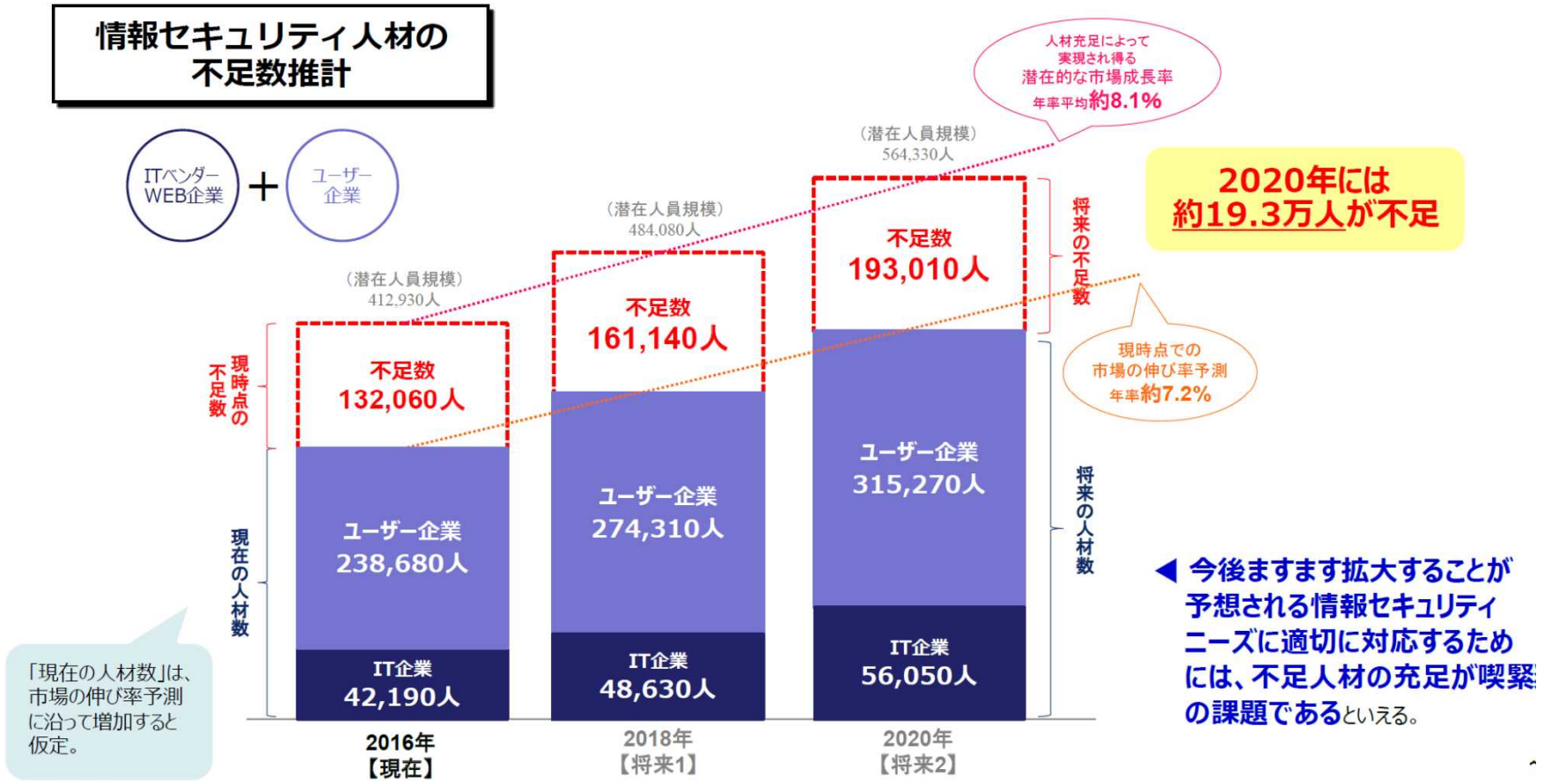
（出典）総務省　情報通信白書　（平成29年）

2030年までのIoT・AIの経済成長へのインパクト（市場規模）



（出典）総務省「IoT時代におけるICT経済の諸課題に関する調査研究」（平成29年）

サイバーセキュリティ人材の規模



出典：経済産業省　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）

各省庁の人材育成施策
（平成30年度概算要求関連資料）

総務省

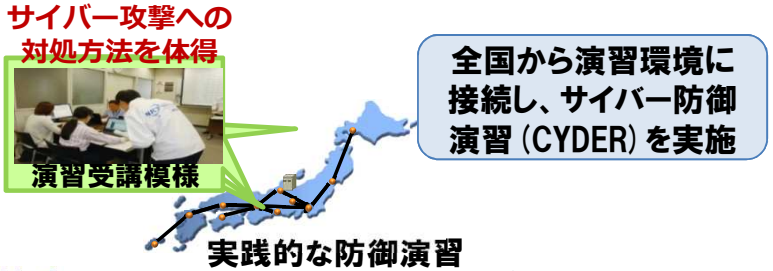
セキュリティ人材の育成（ナショナルサイバートレーニングセンター）

○　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年に国立研究開発法人情報通信研究機構（NICT）に組織した「ナショナルサイバートレーニングセンター」において、下記取組を実施。

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企業等に対するサイバー攻撃について、実践的な防御演習を実施 （CYDER）

② 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セキュリティ人材の育成（サイバーコロッセオ）

③ 若手セキュリティエンジニアの育成 （SecHack365）



東京大会に向けた人材育成

若手セキュリティエンジニアの育成

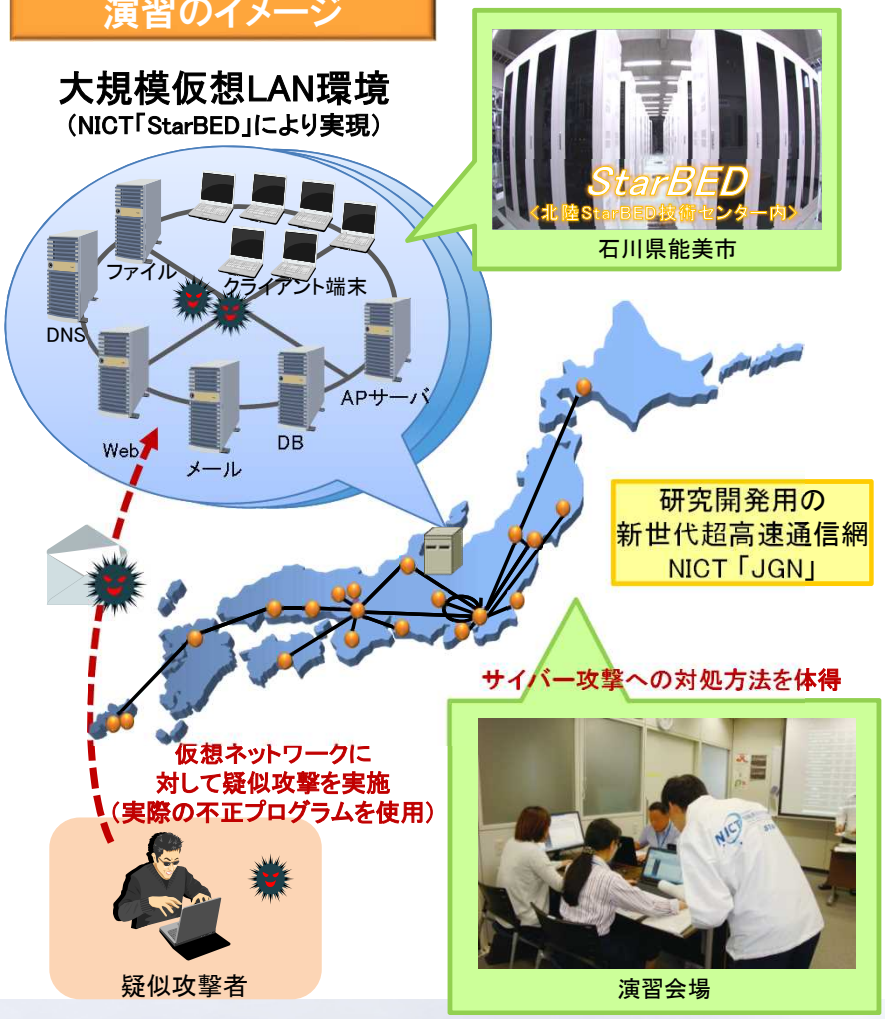
平成30年度要求額　17億円

総務省

実践的サイバー防御演習（CYDER）

CYDER: CYber Defense Exercise with Recurrence

演習のイメージ



演習の特徴

- サイバー攻撃が発生した場合の被害を最小化するための一連の対処方法（攻撃を受けた端末の特定・隔離、通信記録の解析による侵入経路や被害範囲の特定、同種攻撃の防御策、上司への報告等）を体得
- 150台の高性能サーバを用いた数千人規模の仮想ネットワーク環境（国の行政機関や大企業を想定）上で演習を実施
- 我が国固有のサイバー攻撃事例を徹底分析し、最新の演習シナリオを用意

平成29年度の実施内容

演習規模を拡大し、全国47都道府県において約3000人を目標に実施中

総務省

2020東京大会に向けたサイバー演習（サイバーコロッセオ）

○ 2020年東京オリンピック・パラリンピックを想定した大規模演習基盤による演習を実施。

イメージ図

攻防戦によるサイバー演習

具体的内容

- 大規模クラウド環境を用いて、公式サイト、大会運営システム、社会インフラの情報システム等を模擬したシステムを構築。
- 当該システムにより、大会開催時に想定されるサイバー攻撃を再現し、大会組織委員会のセキュリティ担当者を中心に、攻撃・防御手法の検証及び訓練を行う。

大規模な演習を実施し、2020東京大会のサイバーセキュリティを確保

総務省

若手セキュリティエンジニア育成プログラム（SecHack365）

○　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が若年層のICT人材を対象に、自身の持つサイバーセキュリティの研究資産を活用し、実地研修及び遠隔開発による年間プログラムを提供。

実地研修の様子

対象者

・　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。平成30年度も同程度を想定。）

文科省

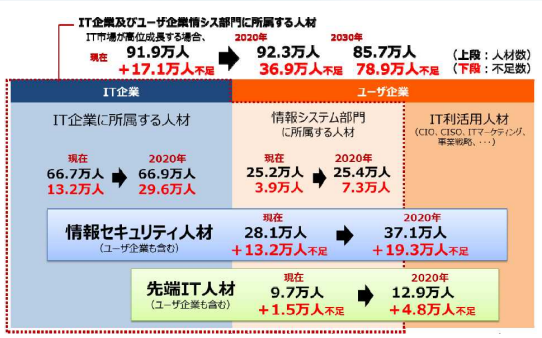
Society 5.0に対応した高度技術人材育成事業

平成30年度概算要求額　20億円(９億円)

背景・課題

◆ 第四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）

施策・提言等

【未来投資戦略2017―Society 5.0 の実現に向けた改革―】
平成29年6月9日閣議決定(抄)

第2 具体的施策
Ⅱ Society 5.0に向けた横割課題
A. 価値の源泉の創出
3. 人材の育成・活用力の強化
ⅰ)個々の働き手の能力・スキルを向上させる人材育成・人材投資の抜本拡充
②実践的な能力・スキルを養成するための産官学連携したシステムの構築
③大学等の高等教育機関が「IT・データスキル」育成の重要なプレーヤーとなるための制度改正・政策支援
④「社会人の生涯学び直し」における「IT・データスキル」等育成の抜本拡充

【世界先端IT国家創造宣言・官民データ活用推進基本計画】
平成29年5月30日閣議決定(抄)

第2部　官民データ活用推進基本計画
Ⅰ-2具体的施策
Ⅱ―1―(9)　人材育成、普及啓発等
①分野横断的な施策のうち重点的に講ずべき施策
・AI、IoT 等を有効に活用するために不可欠なデータ活用に係る専門的な知識や技術を有する人材の育成について、政府一体となって計画的に実施
・不足するセキュリティ・IT 人材の計画的な育成
・社会人の学び直しの推進(技術系人材の再教育)

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。

事業の取組内容

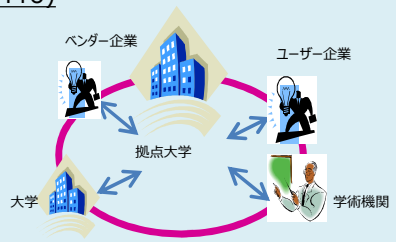
取組①成長分野を支える情報技術人材の育成拠点の形成(enPiT)

１４億円(９億円)【拡充】

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。

◆ 学部学生に対する実践的教育の推進(enPiTⅡ)
（運営拠点：１拠点、分野別中核拠点：４拠点）
・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
・産業界と協力な連携体制を構築

◆ IT技術者の学び直しの推進(enPiT-Pro)
（４拠点 ⇒ ９拠点(対前年度＋５拠点)）
・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を加速

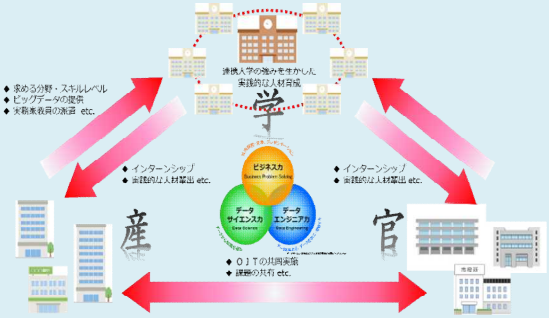


取組②超スマート社会の実現に向けたデータサイエンティスト育成事業

６億円【新規】

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数理科学の応用展開を図り、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（６拠点整備）
・大学間連携により、PBL中心の実践的な教育を実施
・産業界と協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
・拠点間で連携し、データを取扱う際のガイドラインを策定する等の人材育成システムを全国に普及



文科省

社会ニーズを踏まえた新分野・領域教育の推進

「情報セキュリティ人材」(継続)

平成30年度概算要求額：648億円の内数（前年度予算額：623億円の内数))
((独)国立高等専門学校機構運営費交付金　特別教育研究経費の内数)

1．課題・背景

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、情報セキュリティ人材の育成が急務となっている。

2．取組概要

（1）高知高専、石川高専などにおいて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を行う。【継続事業】

（2）情報セキュリティに関する知識やスキルの習得に加え、高い倫理観やITリテラシーを習得する教材・教育プログラムの展開と、社会ニーズを踏まえた実践的な演習環境の高度化を図る等、教育環境を加速度的に整備することにより、情報セキュリティ人材の質的向上と量的拡大を図る。【拡充事業】

「セキュリティ演習拠点」の整備【拡充事業】

◇ 「情報セキュリティ人材」の演習拠点を全国10ヶ所に整備し、いずれかで常に最新のソフトウェア等を備え、全国の高専からアクセスを可能としたサイバーレンジ（実践的な演習環境）を提供

○ 第１フェーズ：平成28年度に整備した先行５拠点において、「情報セキュリティ人材」の育成に必要な教育実践を検証し、理想的な環境整備と実効性のある教育方法を確立させる。

○ 第２フェーズ：第１フェーズで構築したものを基に、全高専を補完するため、後発５拠点の教育環境整備を実施し、全国10ヶ所で「情報セキュリティ人材」の発掘・育成を強力に実行する。

※ 日々進化しているサイバー攻撃技術にも対応するため、全国10ヶ所のいずれかで、常に最新のソフトウェア等を備えることとし、４年周期で環境更新を行う。

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

《第１フェーズ（H28’）》

5拠点 ⇒ 10拠点
（検証）　（展開）

《第２フェーズ（H29’）》

【拠点整備・環境更新の年次計画イメージ】

◎ 拠点整備 ⇒ 平成28年度、29年度の2カ年で整備

◎ 環境更新 ⇒ 平成30年度から４年周期で更新

	H28’	H29’	H30’	H31’	H32’	H33’	H34’	H35’・・・
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	3拠点	2拠点・・・

文科省

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。

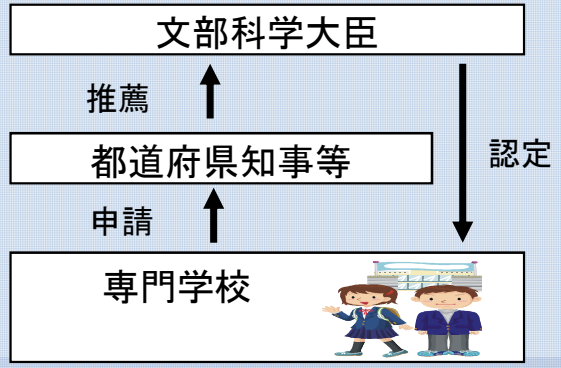
⇒平成25年8月　「専修学校の専門課程における職業実践専門課程の認定に関する規程(文部科学省告示第133号)」を公布・施行

⇒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**として位置づけることが必要。

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

情報モラル教育の推進

子供たちをとりまく環境等の現状

- 2010年前後からスマートフォンやSNSが子供たちの間にも急速に普及
- インターネット利用が長時間化、コミュニティサイト等での被害の増加
- 他者の個人情報の取扱いや不正請求等の危険への対処に課題（平成25年度「情報活用能力調査（小・中学校）」）

「情報モラル」とは（学習指導要領解説総則編）

「情報社会で適正な活動を行うための基になる考え方と態度」

- 他者への影響を考え、人権、知的財産権など自他の権利を尊重し情報社会での行動に責任をもつこと
- 危険回避など情報を正しく安全に利用できること
- コンピュータなどの情報機器の使用による健康とのかかわりを理解すること　など

情報モラル教育の進め方（3つの視点）（指導の手引き）

- ➢日常モラルを育てる
- ➢仕組み（インターネットや機器・サービス等の特性）を理解させる
- ➢日常モラルと仕組みを組み合わせて考えさせる

情報モラル教育充実の視点（例）

- ✓ 情報端末の使用の安易な禁止ではなく、より適切に使用できるようにする
- ✓ 狭義のモラルだけでなく、情報安全や情報セキュリティを含む情報モラル教育に取り組んでいく
- ✓ 「なぜしてはいけないのか」「なぜしなければならないのか」を考えさせる（道徳的に考えるだけでなく、発達の段階に応じて、情報や情報技術の特性も踏まえて考えさせる）
- ✓ 学校全体で計画的に取り組み、その上で必要に応じて生徒指導と連携するとともに、家庭や地域とも連携していく

主な取組

■『情報社会の新たな問題を考えるための教材～安全なインターネットの使い方を考える～』動画教材と手引書
（平成25年度作成、27年度改訂・充実）

すぐに授業に活用できるようモデル指導案、ワークシート例、アンケート例等を添付

■『保護者のための情報モラル教室 話し合っていますか？家庭のルール ～安全で安心なインターネット利用のために～』動画教材、パンフレット等
（平成27年度作成）

PTAの集会等、保護者の方を対象とした様々な場で活用できる教材

■『情報モラル実践事例集2015』
（平成27年度作成）

教育委員会、学校のほか、地域が主体となって取り組んだ実践事例を紹介

http://www.mext.go.jp/a_menu/shotou/zyouhou/detail/1369617.htm

■教員等を対象としたセミナー・フォーラムの実施

経産省

産業系サイバーセキュリティ推進事業

商務情報政策局　サイバーセキュリティ課
03-3501-1253

平成30年度概算要求案　２１．０億円（１１．７億円）

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

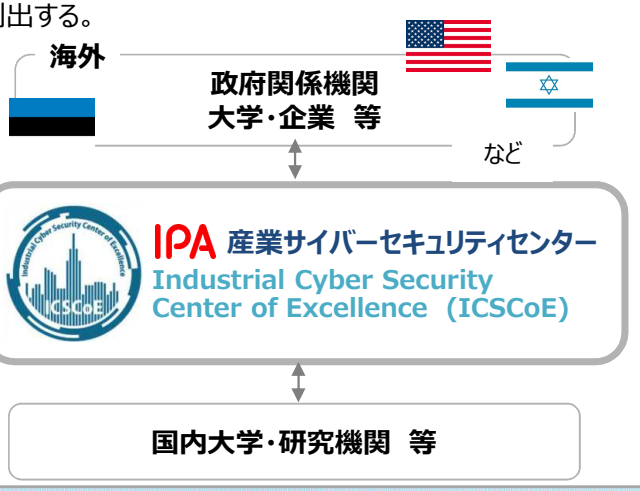
事業イメージ

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。



経産省

独立行政法人情報処理推進機構（IPA）運営費交付金

商務情報政策局
総務課　03-3501-2964
ｻｲﾊﾞｰセキュリティ課　03-3501-1253
情報技術利用促進課　03-3501-2646
情報産業課　03-3501-6944

平成30年度概算要求額 52.9億円（45.4億円）

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）ITが社会各層に浸透したことに伴う情報セキュリティ対策の強化

重要インフラや企業等に対するサイバー攻撃に関する情報などの収集・評価・分析を行うとともに、対策方法の提案・普及を通じて、被害の未然防止や低減を図ります。

（２）高度なIT人材の発掘・育成・支援とIT人材の裾野の拡大

未踏IT人材発掘・育成事業の実施及び拡充等を通じて高度なIT技術を有する人材への支援を強化するとともに、このような人材の起業・事業化に向けた支援を強化します。また、試験制度の着実な実施・普及等によりIT人材の裾野の拡大に取り組みます。

（３）社会基盤としてのＩＴ技術の実装支援に向けた取組

国民・企業が、IT技術の進化に伴う利益を有効かつ安全に享受できるよう、常に最先端の技術動向の調査分析を行い、それらを役立つ形で発信します。

成果目標

- 国家資格「情報処理安全確保支援士」について、2020年までに３万人超の有資格者の確保を目指すという政府目標に貢献します。
- 未踏IT人材発掘・育成事業等を通じ、チャレンジ精神溢れ将来の起業へとつながる人材を年間 100 名輩出することを目指すという政府目標に貢献します。

条件（対象者、対象行為、補助率等）

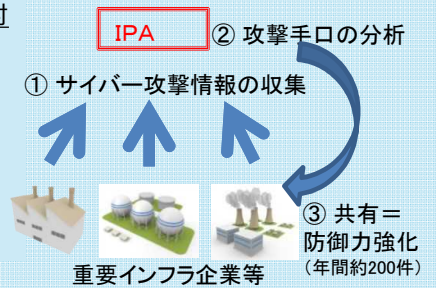
国 → 交付金 → 情報処理推進機構（IPA）

事業イメージ

（１）ITが社会各層に浸透したことに伴う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。



（２）高度なIT人材の育成・支援とIT人材の裾野の拡大

- 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クリエータを発掘・育成します。また、産業界をリードするIT等のトップ人材を創出するため、事業化・起業支援の人材育成プログラムを創設し、日本の将来を切り拓いていくIT人材の発掘・育成を強化します。


（未踏人材発掘・育成事業）

- セキュリティ・キャンプ

若手のセキュリティ人材に対し、第一線の技術者が最新のノウハウ等を伝授します。

（３）社会基盤としてのIT技術の実装支援に向けた取組

- ＩＴ技術の動向に関する情報収集・発信等

AIをはじめとした最先端のIT技術の動向を情報収集・調査・分析しつつ、国民・企業の役に立つ形で発信します。

- ＩＴに関するタスクとスキルの体系化

ITを利活用するビジネスに求められる業務（タスク）と、それを支えるIT人材の能力や素養（スキル）を体系化します。

金融庁の施策例

金融分野のサイバーセキュリティ対策強化

○ 金融業界横断的なサイバーセキュリティ演習の実施

平成３０年度概算要求：0.6億円（平成29年度当初予算：0.５億円）

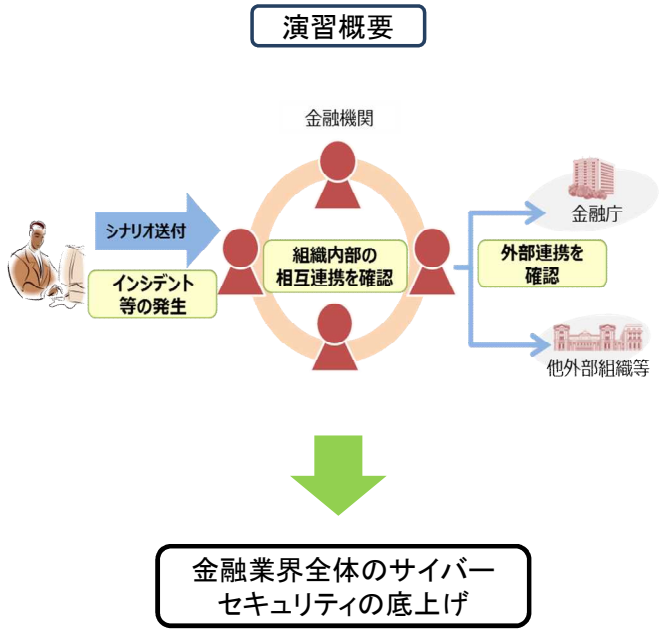
事業概要

- 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29年度、２回目の「金融業界横断的な演習」（Delta Wall Ⅱ）を実施予定。

（参考）平成29年度演習においては、中小金融機関の底上げを目的に、参加金融機関の参加枠および対象業態を拡充のうえ、約100先が参加予定（前回は77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３０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）



警察の施策例

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、鉄道、電力、ガス、
政府・行政サービス、医療、水道、物流、
石油、クレジット、化学**

（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。

障害対応体制の強化

重要インフラ事業者における重要インフラサービス障害対応の実態や演習ニーズに適合した演習・訓練の充実による重要インフラ防護能力の維持・向上。

現状の課題

- より効果的で実用的な分野横断的演習の企画推進
- 参加者拡大や、重要インフラサービス障害発生時の関係主体間の在り方に適合した演習成果の普及・浸透

行動計画期間中の施策

（１）分野横断的演習の継続と改善

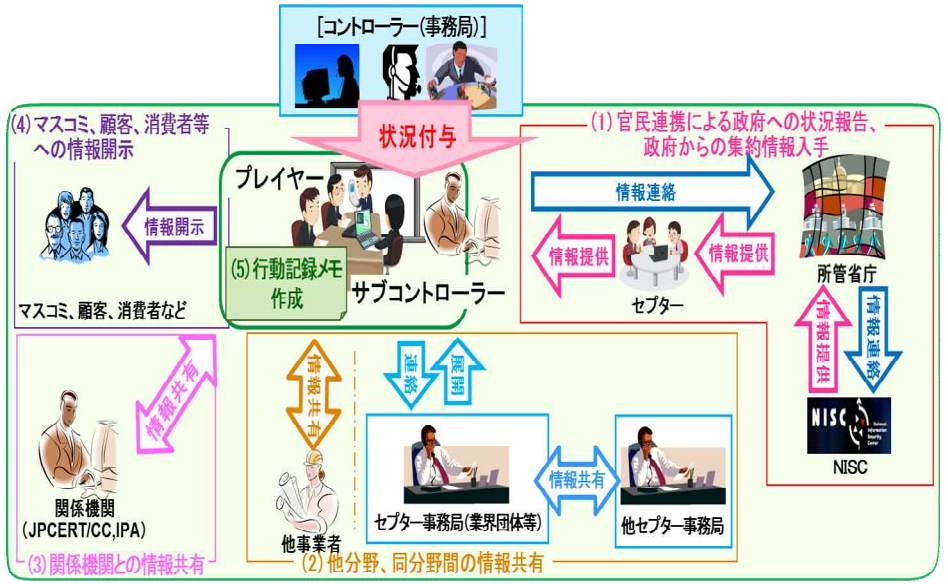
- 重要インフラ事業者の実態に即した演習企画
  - ・重要インフラ事業者の演習ニーズ取り込み
  - ・最新の攻撃手法を考慮した演習シナリオ整備
  - ・外縁の事業者や密接に関連する関係主体の参画

（２）参加者大幅増に即した演習成果の浸透

- 新規参加への促進
- 他演習・訓練との相互連携
- 経営理解増進に寄与する演習企画
- 自社演習実施に資する演習ノウハウの還元
  - ・仮想的な演習環境の提供　等

第４次行動計画に基づく取組

分野横断的演習の概要（ステークホルダー相関図）



分野横断的演習の継続と充実

- より実態に即した演習企画
- 外縁の事業者も含めた新規参加の促進
- 他演習・訓練との相互連携
- 経営理解増進に資する演習企画
- 演習ノウハウの還元

重要インフラ防護能力の維持・向上