経済産業省

資料２－５

産業サイバーセキュリティ研究会WG2における
サイバーセキュリティ人材政策に関する議論の状況について

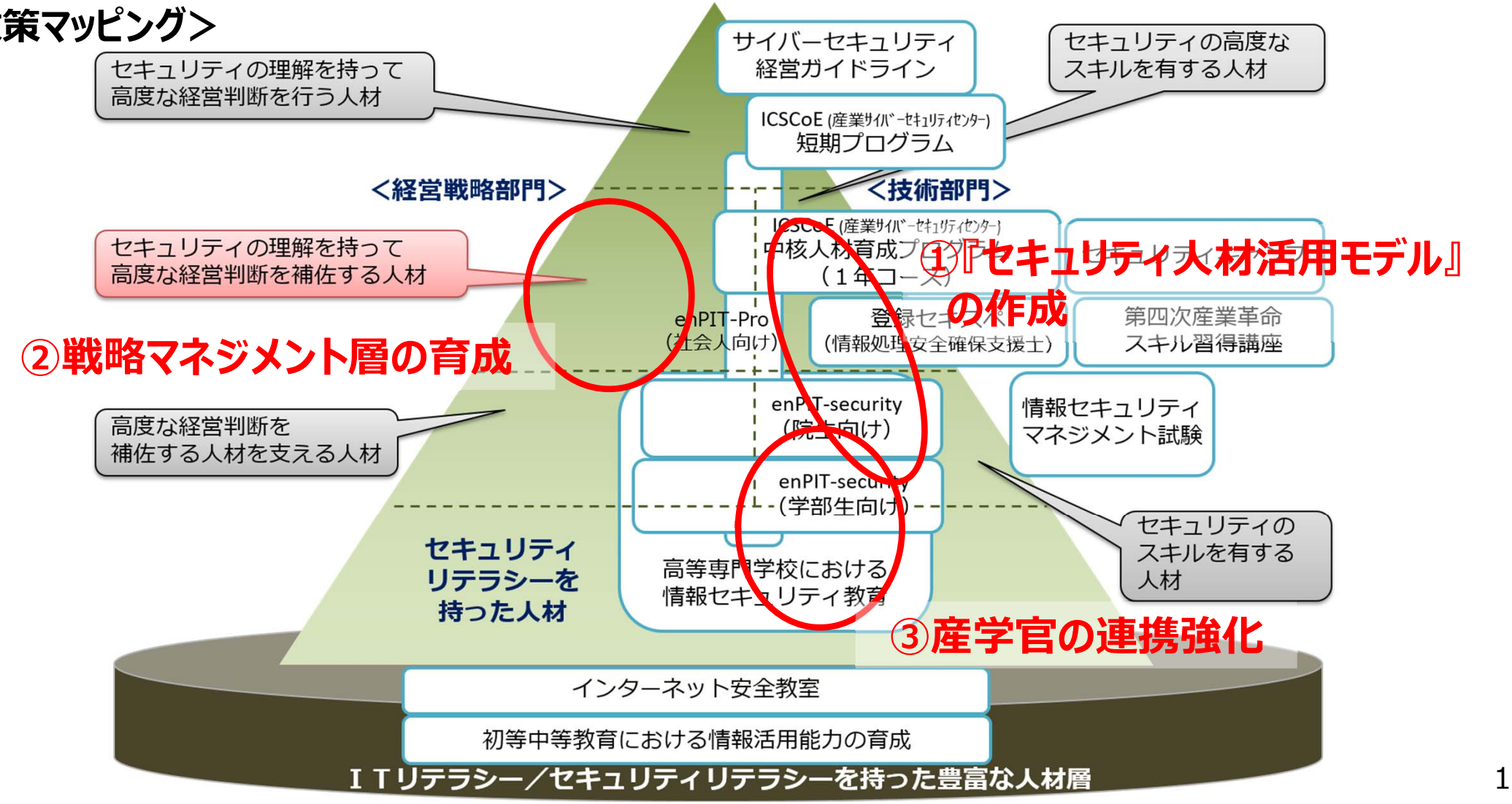
経済産業省
商務情報政策局

サイバーセキュリティ人材育成・活躍促進パッケージの全体像

第二回産業サイバーセキュリティ研究会資料より再掲

- ユーザー企業において必要となる**セキュリティ人材の定義、評価指標が不明確。**
- **「セキュリティの理解を持って高度な経営判断を補佐する人材」の育成が不十分。**
- 教育プログラム策定への貢献など、**産業界の教育への取組の強化が期待される。**

＜政策マッピング＞



（参考）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

- 2017年5月の「連邦政府の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、米国の商務省・国土安全保障省が共同で、サイバーセキュリティ人材の育成に関する大統領への報告書を策定（2017年11月）、公表（2018年5月）。

(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と併せ、事業分野に関する知識・スキルも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。

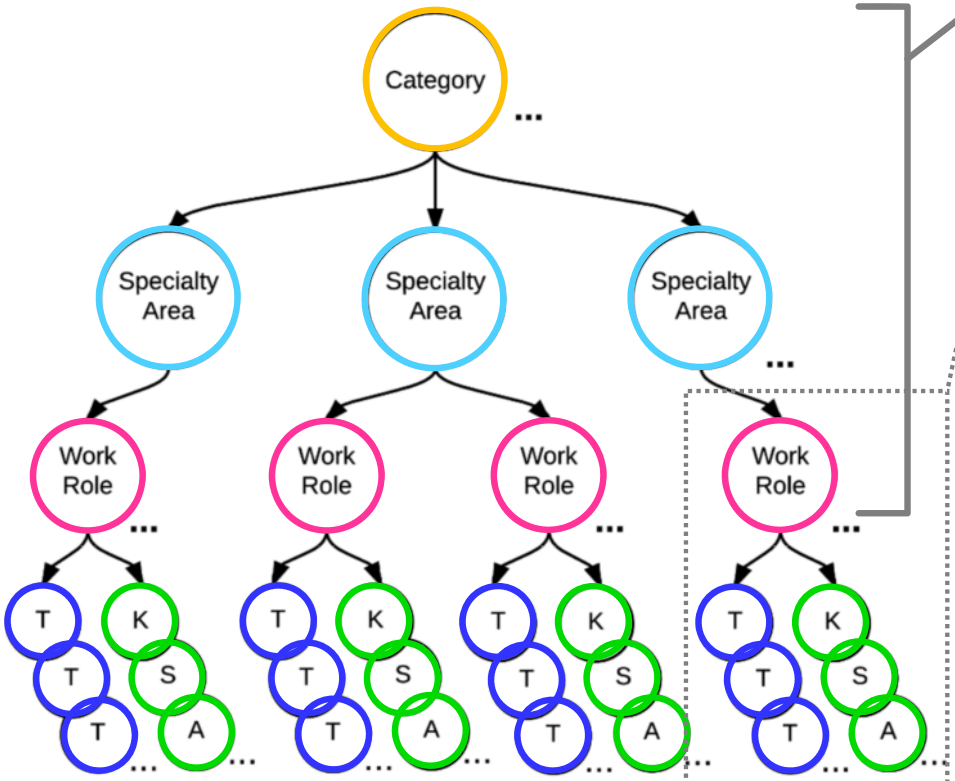
(3) 推進すべき主な取組

➢ 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

(参考) NICE (National Initiative for Cybersecurity Education) Cybersecurity Workforce Framework (SP800-181)

- NIST（国立標準技術研究所）が中心となり産学官で策定したサイバーセキュリティ人材に関するフレームワーク。（2013年4月策定、2017年8月改訂）
- サイバーセキュリティ業務に関する52種類の役割と、各役割に求められるタスクや知識・技能・能力の関係を明確化。

＜NICEフレームワークの構成＞



タスク: 1007項目　**スキル**: 374項目
知識: 630項目　**能力**: 176項目

7種類の**カテゴリ**、33種類の**専門分野 (Specialty Area)**、52種類の**役割 (Work Role)** から構成

各役割には、達成される**作業(T:Task)**と、役割を果たすために必要な**知識 (K:Knowledge)**、**技能 (S:Skill)**、**能力 (A:Ability)** が紐付いている

Work Roleの例（Authorizing Official）

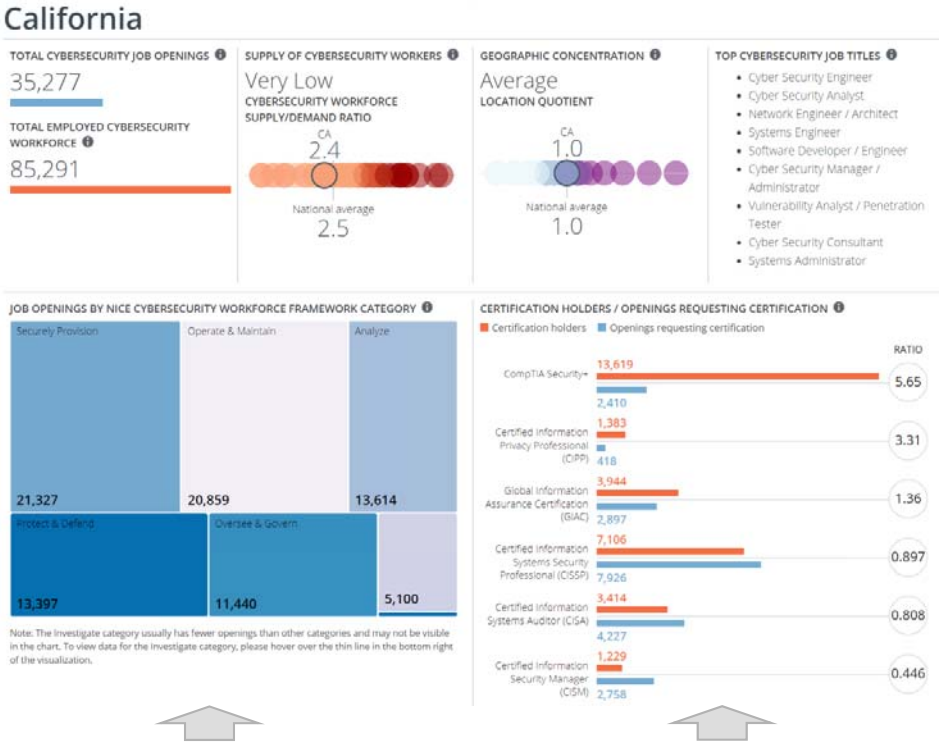
Work Role Name	Authorizing Official
Work Role ID	SP-RSK-001
Specialty Area	Risk Management (RSK)
Category	Securely Provision (SP)
Work Role Description	Senior official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation (CNSSI 4009).
Tasks	T0145, T0221, T0371, T0495
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0013, K0019, K0027, K0028, K0037, K0038, K0040, K0044, K0048, K0049, K0054, K0059, K0070, K0084, K0089, K0101, K0126, K0146, K0168, K0169, K0170, K0179, K0199, K0203, K0260, K0261, K0262, K0267, K0295, K0322, K0342, K0622, K0624
Skills	S0034, S0036
Abilities	A0028, A0033, A0077, A0090, A0094, A0111, A0117, A0118, A0119, A0123, A0170

T0495	Manage Accreditation Packages (e.g., ISO/IEC 15026-2).
K0267	Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures.
S0367	Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).
A0170	Ability to identify critical infrastructure systems with information communication technology that were designed without system security considerations.

出典： NIST SP800-181

（参考）NISTによるCyberSeekプロジェクト

- NIST（国立標準技術研究所）が支援するオンラインサイト。米国の各地域におけるオンライン求人状況等の情報を、NICEフレームワークや民間団体が提供する資格と紐づけて視覚的に提供。
- 役割とスキルを紐づけ共通言語化することにより、こういった取組が可能になる。

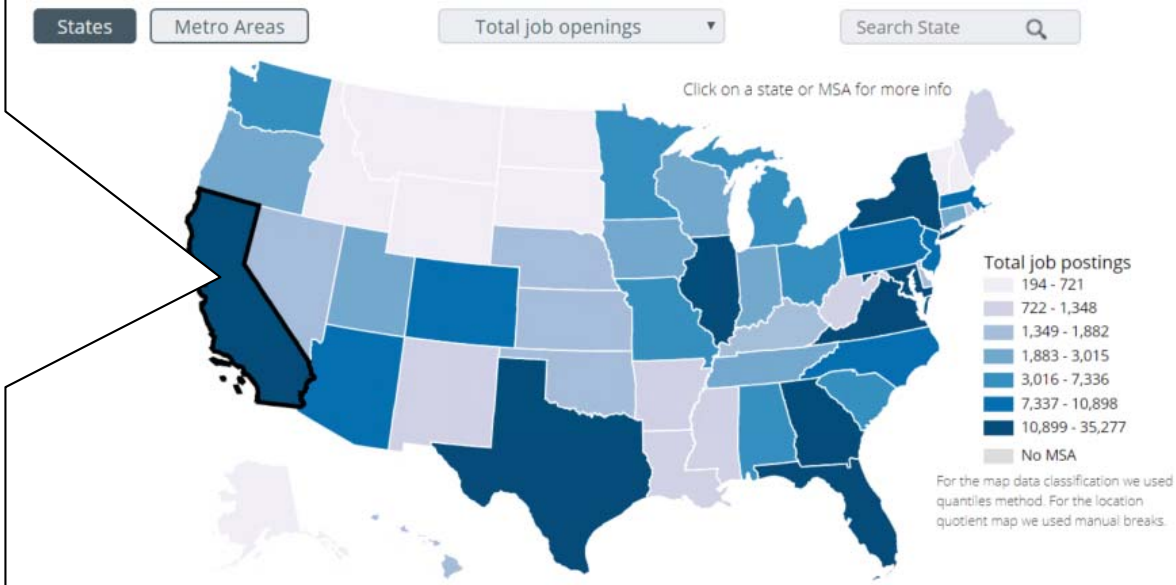


NICEフレームワークの７カテゴリーの分類で求人数を表示。

- Securely Provision
- Operate & Maintain
- Analyze
- Protect & Defend
- Oversee & Govern
- Collect & Operate
- Investigate

民間団体が提供するそれぞれの資格の保有者の数と求人要件となっている数を提示。

上記のカリフォルニア州の例だと、CISSP資格は保有者よりも求人数の方が多いことが分かる。



<プロジェクトパートナー>

NICE NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

→ NISTによるセキュリティ人材に関する産官学のプロジェクト

burningglass CAREERS IN FOCUS

→ 労働市場のデータ分析に強みを持つ民間企業

CompTIA

→ Security+, Network+等のIT資格を開発・提供している業界団体

出典：https://www.cyberseek.org/

サイバーセキュリティ対策を支える基盤となる
サイバーセキュリティ人材育成・活躍促進パッケージ

①『セキュリティ人材活用モデル』の作成

- 役割定義の整理
- 委託調査

② 戦略マネジメント層の育成

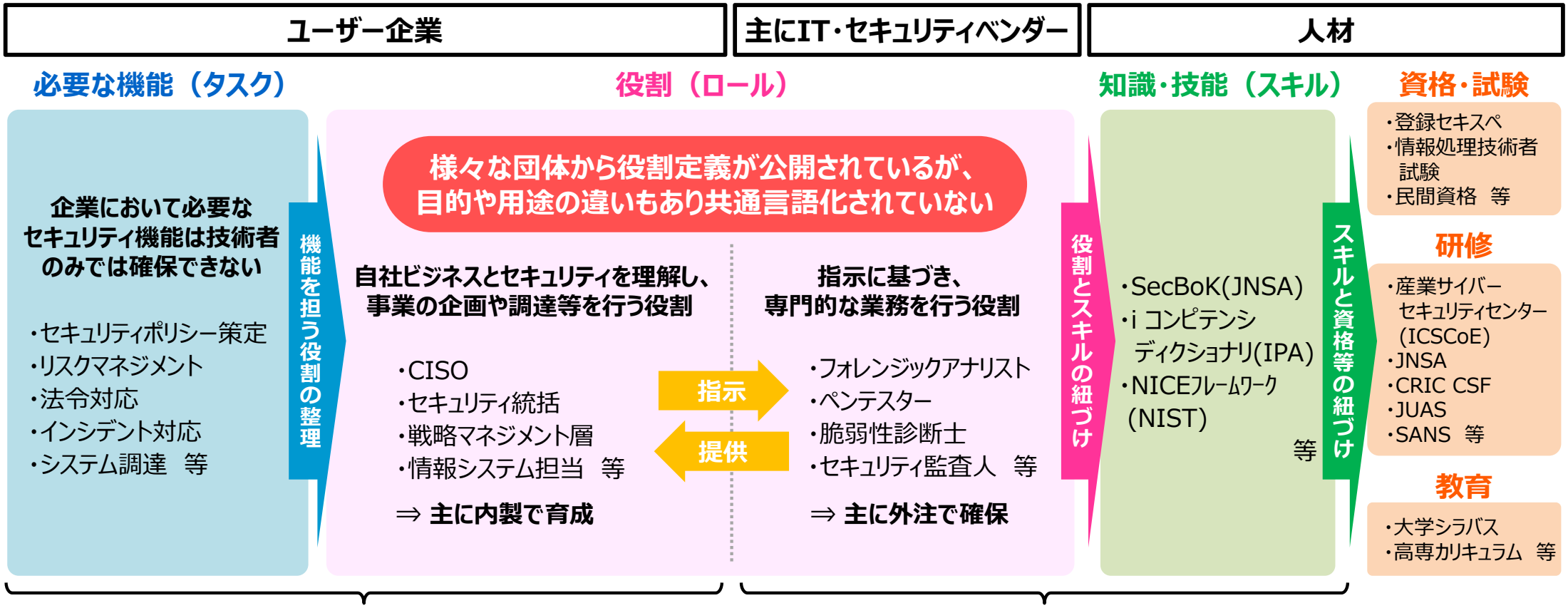
- 育成プログラムの提供

③ 産学官の連携強化

- 高専との連携の具体化
- 地域的取組の促進

セキュリティ人材の流動化に対応できる『セキュリティ人材活用モデル』の構築

- 企業に求められるセキュリティ機能を果たす人材の役割（肩書き）を、必要な知識・技能（スキル）と紐づけ、共通言語化することにより、人材の雇用・配置・外注等における企業と人材の間のコミュニケーションコストを減らし、マッチングを促進。
- 人材のニーズとシーズの見える化により、セキュリティ人材の最適活用、処遇改善につなげる。



論点1　ユーザー企業によって機能・体制・役割の在り方は様々

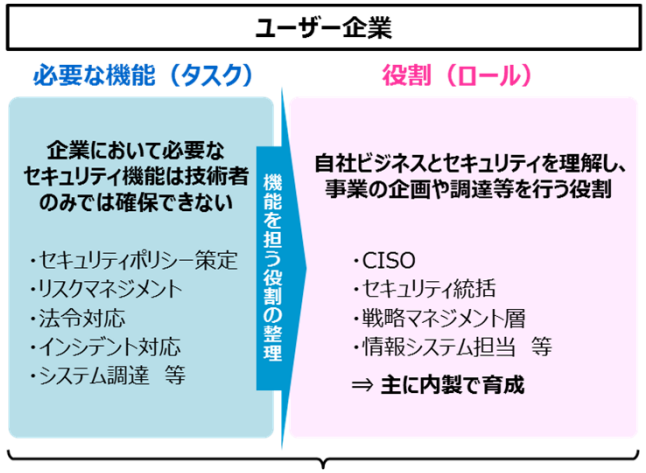
⇒ ユーザー企業の規模・業種・成熟度等に応じたセキュリティ体制や人材確保の関係について調査を実施

論点2　専門性が高い役割は比較的共通言語化しやすい

⇒ SecBoK(JNSA)、ITSS+(METI/IPA)、統合セキュリティ人材モデル(サイバーセキュリティ人材育成スキーム策定共同プロジェクト)等における既存の役割定義・専門分野の関係を整理・明確化

ユーザー企業におけるセキュリティ体制・人材確保に関する調査の実施

- 29年度の調査では、米国・英国のCISO等に対し、人材の確保・配置状況や企業のセキュリティ体制の成熟度等に関するアンケートを実施。成熟度を高める上で効果的な取組は、企業規模に応じて異なる可能性がある。
- 30年度の調査では、規模・業種・成熟度等に応じた様々なセキュリティ体制や人事・教育体制が存在する国内ユーザー企業を対象にヒアリング等を実施し、セキュリティ担当と事業部門の連携の在り方や、セキュリティ担当や戦略マネジメント層等のキャリアパス・活躍イメージ（ロールモデル）等、企業が人材戦略を考える上で参考となるプラクティスを抽出。



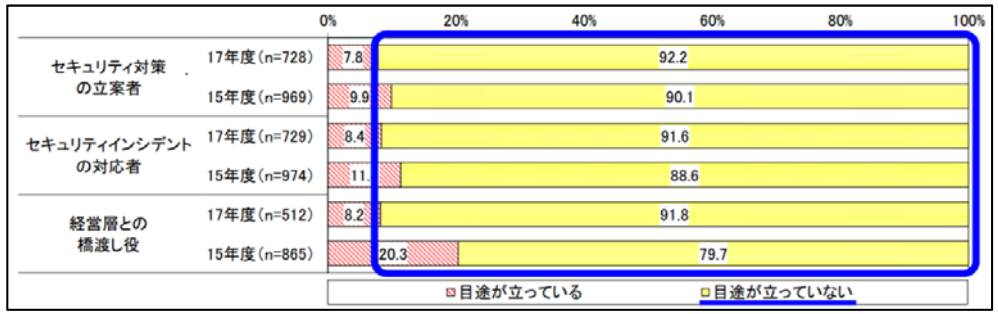
論点1 ユーザー企業によって機能・体制・役割の在り方は様々

⇒ ユーザー企業の規模・業種・成熟度等に応じたセキュリティ体制や人材確保の関係について調査を実施

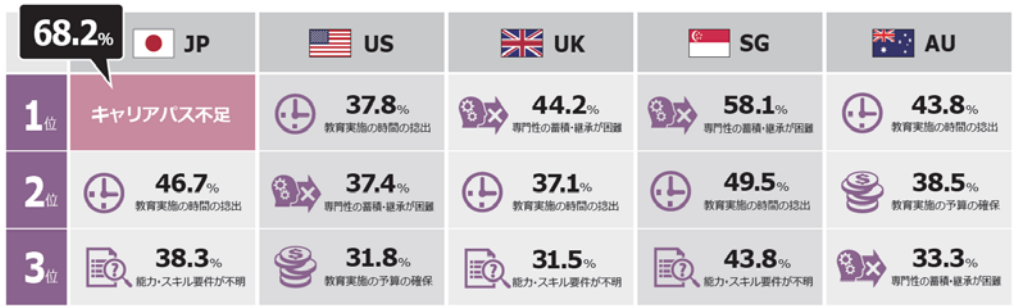
＜委託調査の概要＞

- ユーザー企業に対するヒアリング（30社程度）により、企業の規模・業種・成熟度等と組織体制・人材確保の関係について調査
- セキュリティ担当と事業部門の連携の在り方に関するプラクティスを抽出
- セキュリティ担当・戦略マネジメント層等のキャリアパス（ロールモデル）を抽出
- 海外動向等文献調査
- 有識者ヒアリング（10名程度）
- 報告書の作成

（背景１）日本の多くのユーザー企業では、内製すべきセキュリティ人材が不足。（背景２）人材育成・教育に係る課題のうち、日本ではキャリアパス不足が突出。



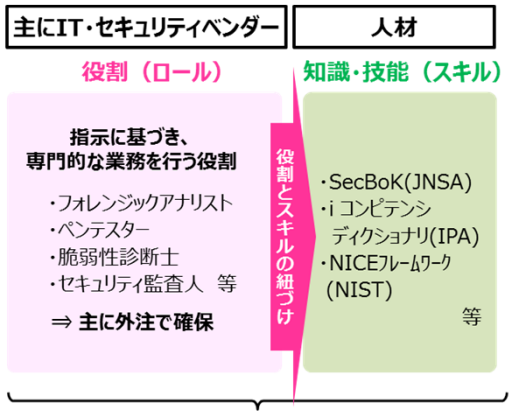
出典：(一社)日本情報システム・ユーザー協会『企業IT動向調査2018』
（ユーザー企業 1,078社に調査）



出典：NRIセキュアテクノロジーズ株式会社『NRI Secure Insight 2018』
（ユーザー企業 計1,110社に調査）

専門性が高い分野における役割定義の関係整理

- 専門性が高い役割については、比較的共通言語化しやすいと思われるが、目的や用途に応じ、様々な役割定義が存在。
- NICEフレームワーク等の海外の規格も参照しつつ、国内における既存の様々な役割定義の関係整理に向け、関係団体（IPA、JNSA、産業横断サイバーセキュリティ人材育成検討会（以下、CRIC CSF）等）と継続的に議論を実施。（9月27日、10月26日に、関係団体との議論を実施。）



論点2 専門性が高い役割は比較的共通言語化しやすい

⇒ SecBoK(JNSA)、ITSS+(METI/IPA)、統合セキュリティ人材モデル(サイバーセキュリティ人材育成スキーム策定共同プロジェクト)等における既存の役割定義・専門分野の関係を整理・明確化

目的や用途の違いから、役割の名称・定義の粒度はそれぞれ異なる

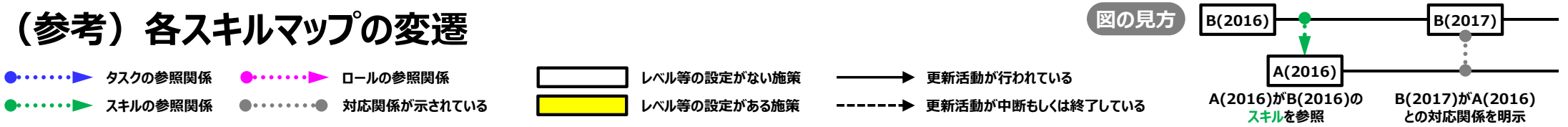
例として、既存のそれぞれの役割定義に沿ってインシデント対応に関係する役割を塗りつぶしたものが右表。

（※なお、塗りつぶし箇所以外にも広い意味でインシデント対応に関係する役割は存在。）

＜各団体による役割・専門分野の定義の例＞

ITSS+（セキュリティ領域）【METI / IPA】	SecBoK【JNSA】	人材定義リファレンス【CRIC CSF】	統合セキュリティ人材モデル【サイバーセキュリティ人材育成スキーム策定共同プロジェクト】	NICEフレームワーク (Specialty Areas)【NIST】
情報リスクストラテジ	CISO	CISO/ CRO/ CIO等	セキュリティコンサルタント	Risk Management
情報セキュリティデザイン	POC (Point of Contact)	サイバーセキュリティ統括（室等）	セキュアシステムプランナー	Software Development
セキュア開発管理	ノーティフィケーション	システム部門責任者	セキュアシステムデベロッパー	Systems Architecture
脆弱性診断	コマンダー	システム管理者	セキュアアプリケーションデベロッパー	Technology R&D
情報セキュリティアドミニストレーション	トリアージ	ネットワーク管理者	セキュリティマネージャー	Systems Requirements Planning
情報セキュリティアナリシス	インシデントマネージャー	CSIRT責任者	セキュリティオーディター	Test and Evaluation
CSIRTキュレーション	インシデントハンドラー	サイバーセキュリティ事件・事故担当	システムリスクアセッサー	Systems Development
CSIRTリエゾン	キュレーター	セキュリティ設計担当	ペネトレーションテスター	Data Administration
CSIRTコマンド	リサーチャー	構築系サイバーセキュリティ担当	ネットワークリスクアセッサー	Knowledge Management
インシデントハンドリング	ソリューションアナリスト	運用系サイバーセキュリティ担当	リサーチャー	Customer Service and Technical Support
デジタルフォレンジクス	セルフアセスメント	CSIRT担当	フォレンジックエンジニア	Network Services
情報セキュリティインベスティゲーション	脆弱性診断士	SOC担当	インテリジェンスアナリスト	Systems Administration
情報セキュリティ監査	教育・啓発	ISMS担当	インシデントレスポンダー	Systems Analysis
	フォレンジックエンジニア	システム企画担当	セキュアオペレーター	Legal Advice and Advocacy
	インベスティゲーター	基幹システム構築担当		Training, Education, and Awareness
	リーガルアドバイザー	基幹システム運用担当		Cybersecurity Management
	IT企画部門	WEBサービス担当		Strategic Planning and Policy
	ITシステム部門	業務アプリケーション担当		Executive Cyber Leadership
	情報セキュリティ監査人	インフラ担当		Program/Project Management
		サーバ担当		Cyber Defense Analysis
		DB担当		Cyber Defense Infrastructure Support
		ネットワーク担当		Incident Responder
		サポート・教育担当		Vulnerability Assessment and Management
		ヘルプデスク担当		Threat Analysis
		監査責任者		Exploitation Analysis
		監査担当		All-Source Analysis
		特定個人情報取扱責任者		Targets
		特定個人情報取扱担当		Language Analysis
		個人情報取扱責任者		Collection Operations
		個人情報取扱担当		Cyber Operational Planning
				Cyber Operations
				Cyber Investigation
				Digital Forensics

（参考）各スキルマップの変遷



名称	概要	2014以前	2015	2016	2017	2018
情報処理技術者試験・情報処理安全確保支援士試験（METI）	**情報処理技術者試験：** 「情報処理の促進に関する法律」に基づき経済産業省が、情報処理技術者としての「知識・技能」が一定以上の水準であることを認定している国家試験。 **情報処理安全確保支援士：** 最新の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。 https://www.jitec.ipa.go.jp/	情報セキュリティアドミニストレータ試験（2001年～2008年） テクニカルエンジニア（セキュリティ）試験（2006年～2008年） 2009年　春試験より 情報セキュリティスペシャリスト試験（2009年～2016年） 2016年　春試験より 情報セキュリティマネジメント試験 2017年　春試験より 情報処理安全確保支援士試験 情報処理安全確保支援士（登録） 支援士の想定業務を専門分野として具体化				
iコンピテンシディクショナリ(iCD)（IPA）	企業において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「タスクディクショナリ」、「スキルディクショナリ」として体系化したもの。 **タスク: 50(大分類)、スキル：4(カテゴリ)** **タスク参照例: 6分類、99種類** https://icd.ipa.go.jp/icd/	CCSF 2007年： 情報処理技術者試験と3スキル標準の統合を企図 2009年： CCSFに準拠した試験体系 CCSF・追補版 2012年：公開 2014年：iCDに名称変更 「情報セキュリティ人材の育成指標等の策定事業(経産省)」成果	6/30 iCD2015 ITSS等で定義される職種とスキルDの職種を対応付け	6/6 iCD2016	iCDのタスク/スキルDを参照 6/20 iCD2017 2017年度で普及活動終了 → タスク/スキルD保持 8/17 iCD2018 ITSS+で定義される専門分野とスキルDを対応付け	
ITSS（METI/IPA）	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。 **タスク: 11職種・35専門分野　※職種は役割ではない** **スキル: 5カテゴリ** https://www.ipa.go.jp/jinzai/itss/download_V3_2011.html	ITSS、ETSS、UISS ITSS：2011年度以降、更新無し UISS：2011年度以降、更新無し ETSS：2013年度から民間移管				
ITSS＋（セキュリティ分野）（METI/IPA）	ITSSが対象としている情報サービスの提供や、ユーザー企業のIS部門に関わっている人材が「セキュリティ領域」等のスキル強化を図るための学び直しの指針として活用。 **専門分野: 13、タスク、スキルはiCDを参照** ※専門分野は専門的なセキュリティ業務の役割の観点により設定 https://www.ipa.go.jp/jinzai/itss/itssplus.html				IT人材の“学び直し”方向性を提示 4/7 ITSS+ ロールの対応関係をマッピング ITSS+（セキュリティ領域）における専門分野とSecBoKの役割（ロール）との関連を明確化	
SecBoK（JNSA）	情報セキュリティに関する業務に携わる人材が身に付けるべき知識とスキルを整理。 **役割: 16、スキル: 400弱** https://www.jnsa.org/result/2017/skillmap/	2003年：情報セキュリティスキルマップとして登場 2007年：SecBoKに名称変更 SecBoK2009以降、更新無し	NICE、iCDの双方に存在しないが、必要と思われるスキルは独自に追加 4/19 SecBoK 2016 ユーザー企業における人材の定義はNCAを参照 ベンダー企業における人材の定義はNRIで活用されているものを参照		8/21 SecBoK 2017	2018年度内 SecBoK 2018
CSIRT人材の定義と確保（NCA）	各企業のCSIRTにおいて必要な機能、体制、人材を明確化。 **機能: 4、役割: 15** **各役割ごとに任用前提/追加教育スキルを定義** http://www.nca.gr.jp/activity/imgs/recruit-hr20170313.pdf	2014年10月 CSIRT人材WG設立 11/16 Ver. 1.0	SecBoKの16の役割から、開発系を抜いた13の役割を参照		3/13 Ver. 1.5	
NICEフレームワーク（NIST）	サイバーセキュリティ業務の役割・専門分野と必要とされる知識・能力に関する共通言語と分類法を提供。 **7種類のカテゴリ、33専門分野に紐づくロール: 52** **各ロールに以下が紐づく** **タスク: 1007、スキル: 374、知識: 630、能力: 176** https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework	2010年 NICE立ち上げ 2013年4月 Ver. 1.0 2014年4月 Ver. 2.0			8月 Ver. 3.0	NICEフレームワークの改訂に適合
人材定義リファレンス（CRIC CSF）	企業におけるサイバーセキュリティ対策に必要とされる機能を明らかにし、それらの機能を遂行するために必要な人材が果たす役割を定義。 **機能: 29、役割: 30（IT領域）** **対応するスキルセットを定義** http://cyber-risk.or.jp/sansanren/xs_20160914_01_Report_1.0.pdf	2014年10月 経団連傘下に「サイバーセキュリティに関する懇談会」発足 2015年2月 経団連「サイバーセキュリティ対策の強化に向けた提言」公開 2015年6月 提言を受け「産業横断サイバーセキュリティ人材育成検討会（CSF）」が発足	9/14 人材定義リファレンス（IT領域） タスク、ロールは独自に定義	2017年4月 CSFを（一社）サイバーリスク情報センター（CRIC）の委員会として組織改編	11/21発表予定 人材定義リファレンス（OT領域） NICEフレームワークが定めるセキュリティ対策への対応がベース	
統合セキュリティ人材モデル（サイバーセキュリティ人材育成スキーム策定共同プロジェクト）	セキュリティ事故対応やサイバー攻撃監視などといった、各セキュリティ人材として習得すべきスキルセットを体系化し、共通的に利用できる統合セキュリティ人材モデルを策定 **役割: 14、対応するスキルセットを定義** https://jpn.nec.com/press/201810/20181024_03.html				2017年1月 NEC、富士通、日立の3社で検討開始 2017年12月 プロジェクト発足(ニュースリリース)	10/24 統合セキュリティ人材モデル

サイバーセキュリティ対策を支える基盤となる
サイバーセキュリティ人材育成・活躍促進パッケージ

① 『セキュリティ人材活用モデル』の作成

- **役割定義の整理**
- **委託調査**

② 戦略マネジメント層の育成

- **育成プログラムの提供**

③ 産学官の連携強化

- **高専との連携の具体化**
- **地域的取組の促進**

サイバーセキュリティ経営を進める戦略マネジメント層育成の取組み状況

- IPA産業サイバーセキュリティセンターにおいて、企業におけるリスク管理に関わる責任者クラス向けに「戦略マネジメント系セミナー」を本年11月から実施。
- 一橋ビジネススクールICSの協力で、カリキュラムにサイバーセキュリティを組み込んだ「デジタル・トランスフォーメーション時代における経営人材育成プログラム」を本年9月から実施。

	産業サイバーセキュリティセンター「戦略マネジメント系セミナー」	一橋ビジネススクールICS協力「デジタル・トランスフォーメーション時代における人材育成プログラム」
対象者	• CISO、CIOに相当する役割を担っている方 • 総務部門、生産部門等の統括責任者・マネージャークラスの方 • その他、企業においてリスク管理に関わる方全般	• 30代後半～40代の社会人 • 所属組織で次世代の経営を担うことを期待される方 • 現在も経営トップへのアドバイスが期待される方
実施期間	• 平成30年11月～12月（全７回）	• 平成30年9月～（全17回） ※修了式を除く。
カリキュラム	• 「企業におけるサイバーセキュリティ対策の機能」をメインテーマに講義・演習・ケースディスカッションを通じて熟議	• 経営戦略・知識経営等のコアコース • 世界の先進的IT戦略の集中講義 • サイバーセキュリティ、個人情報保護等の講義
受講者実績	• 17名（中核人材プログラム3名を含む。）	• 30名

サイバーセキュリティ対策を支える基盤となる
サイバーセキュリティ人材育成・活躍促進パッケージ

① 『セキュリティ人材活用モデル』の作成

- 役割定義の整理
- 委託調査

② 戦略マネジメント層の育成

- 育成プログラムの提供

③ 産学官の連携強化

- 高専との連携の具体化
- 地域的取組の促進

高専機構と産・官との連携促進・具体化に向けて

- 国立高専におけるセキュリティ教育が産業界の求める人材像とも整合していくためには、産学官の継続的な協力関係が必要。
- このため、高専機構、NISC、経産省、IPA、CRIC CSF、JNSA、JUASが参加し、高専の抱えるニーズに基づき、各関係機関の協力内容を具体化していくための議論をスタート。

＜高専・産・官の対話の場（イメージ）＞

継続的な協力体制

学　高専機構　等
- ■高度セキュリティ人材、情報系人材、非情報系人材
- ■教員　等

産　企業・業界団体
- ■CRIC CSF、JUAS、JNSA
- ■ユーザー企業、IT・セキュリティベンダー　等

ニーズ・シーズの整理・具体化 ▶ 協力の検討 ▶ 産業界に求められるセキュリティ人材の育成・輩出

- ・トップガンの育成支援
- ・キャリア教育
- ・機械・建築・生物等の分野別教材の開発・素材提供
- ・セキュリティ教員向けのFD（Faculty Development）
- ・講師派遣
- ・産業界に求められるセキュリティ人材像の共有
- ・適切なプレイヤーとのマッチング

官　関係省庁・独法等
- ■NISC、文科省
- ■IPA、JPCERT/CC　等

国立高専におけるセキュリティ教育の現状と産学官連携強化の方向性

- 既に開発済みの教材・演習等もあるが、特に応用的内容・分野別のものについては産業界等から協力を得つつ継続的にアップデートされることが望ましい。
- 学生の専攻やセキュリティスキルレベル等によって、求められる教材・演習等やマッチングすべき団体は様々であるため、今後、個別に具体的協力についての議論を深める。

セキュリティスキルレベル

国立高専卒業生
約1万人/年の内訳

約 1 %
トップガンの学生
→ 主に**セキュリティ企業**に就職

約20%
情報系学科の学生
→ 主に**IT企業**に就職

約80%
非情報系学科の学生
→ 主に**ユーザー企業**に就職

KOSEN 国立高等専門学校機構
国立高専教員

文科省予算等で開発された教材・演習等

- 情報モラル教材・情報リテラシー教材（全学科）
- 各専門分野別教材（各学科）
- セキュリティ基礎教材（情報系・一部学科）
- 情報セキュリティ管理者教材（情報系学科）
- 高度人材向け講義教材（情報系学科）
- ・高度セキュリティ合宿（2日間）
  ・KOSENセキュリティコンテスト（2日間）等
- ・情報系教員向け研修（3日間）
  ・高度セキュリティ情報系教員向け研修（半日から1日間）
  ・サイバーセキュリティ演習（90分）等

産・官との連携の具体化の方向性

高専機構のニーズ①：
産業界の第一線で活躍するトップガンやホワイトハッカーからの講義・キャリア教育　等
⇒ IPA、JNSA等と協力の具体化について協議

高専機構のニーズ②：
セキュリティ知識を活かして働くITベンダー社員からのキャリア教育、教材提供　等
⇒ IPA、JNSA、ITベンダー等と協力の具体化について協議

高専機構のニーズ③：
機械・建築・材料・化学等の分野ごとの特徴に応じた教材の開発・素材提供　等
⇒ CRIC CSF、JUAS等と協力の具体化について協議

高専機構のニーズ④：
教員のFaculty Development (FD)
⇒11月15日の情報担当教員向け研修にJPCERT/CCから講師を派遣。IPA、JNSA等と協力の具体化について協議

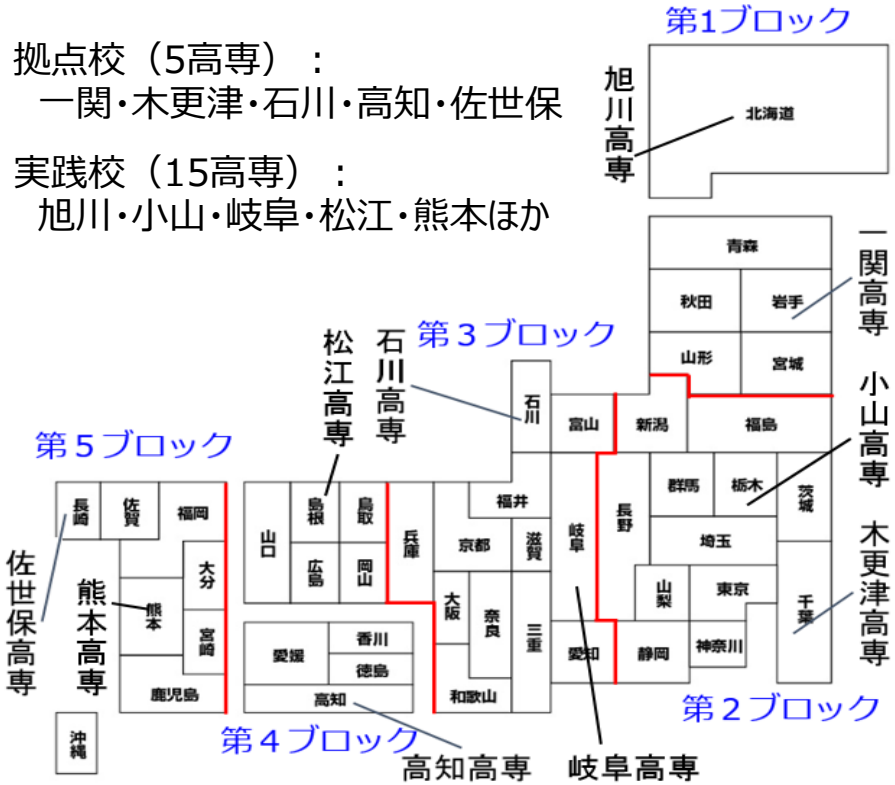
（参考）高専制度の概要

- 高専は、国立51校、公立3校、私立3校が存在。15歳から5年一貫（より高度な教育を実施する専攻科の場合はさらに２年）の技術者教育を行う。
- 各高専ごとに設置されている学科は様々であるが、高知高専等20か所の国立高専において、情報セキュリティ人材の発掘・育成が重点的に実施されている。
- 国立高専では、本科（1～5年生）に約50,000名、専攻科（1～2年生）に約3,000名の学生が在籍しており、毎年約1万人の技術者を輩出。なお、就職先の上位はユーザー企業となっている。

＜国立高専における情報セキュリティ教育重点校＞

拠点校（5高専）：
一関・木更津・石川・高知・佐世保

実践校（15高専）：
旭川・小山・岐阜・松江・熊本ほか



出典：文部科学省提供資料から

＜国立高専生　就職先ランキング（2018年度）＞

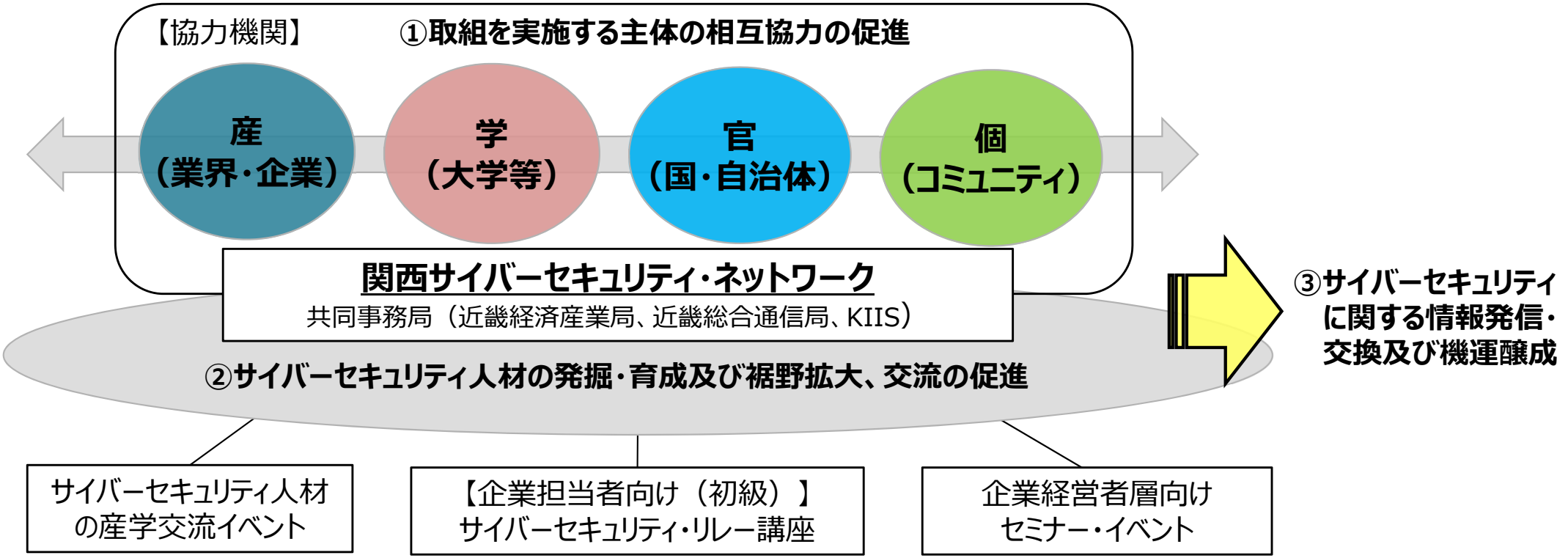
就職先の上位はユーザー企業（非ICT企業）

順位	企業名	採用人数（人）	前年度比（人）
1	JR東海	80	8
2	サントリーグループ（※グループ会社含む）	66	6
3	花王	65	10
4	旭化成	60	8
5	ダイキン工業	57	4
6	三菱電機ビルテクノサービス	49	▲ 3
7	中部電力	48	5
	関西電力	48	2
	JXTGエネルギー	48	2
10	東京ガス	45	4
	メンバーズ	45	14

出典：日経産業新聞　2018年10月19日付
(https://www.nikkei.com/article/DGXMZO36700480191020 18X11000/)より経済産業省作成

地域的取組の推進：関西サイバーセキュリティ・ネットワーク

- 近畿経済産業局、近畿総合通信局、(一財)関西情報センター(KIIS)が共同事務局となり、関西のサイバーセキュリティ人材発掘・育成及び裾野拡大に関心を有する産学官等の相互協力を促進。
- 関西におけるサイバーセキュリティの重要性についての認識の醸成及び情報交換の活性化を図るとともに、人材の発掘・育成及び裾野拡大の円滑化を進める。
- 11月12日にキックオフ。その後、リレー講義、企業経営者層向けセミナー等を実施中。



（参考）関西サイバーセキュリティ・ネットワークの体制

【協力機関】※以下の機関等はあくまで発足時であり、順次拡大を想定。

カテゴリ		主な機関等
産	業界団体・ 経済団体	関西経済連合会、関西経済同友会、大阪商工会議所、神戸商工会議所、京都商工会議所、 関西ものづくりIoT推進連絡会議関係団体（18団体：IT・電気計測器・電子電機・電子部品）、 近畿情報通信協議会、日本ネットワークセキュリティ協会（JNSA）西日本支部、ISACA（情報システムコントロール協会）大阪支部
	セキュリティベンダー	神戸デジタル・ラボ、ファイア・アイ、ラック
	情報通信企業	NTT西日本、オージス総研、NEC、富士通、日立製作所、さくらインターネット
	ユーザー企業	パナソニック、関西電力、大阪ガス、ダイキン工業、毎日放送、朝日放送テレビ、読売テレビ放送
学	大学・大学院	神戸大学、兵庫県立大学、和歌山大学、大阪経済大学、立命館大学情報理工学部上原研究室、 奈良先端科学技術大学院大学サイバーレジリエンス構成学研究室
	研究機関	産業技術総合研究所（AIST）、情報通信研究機構（NICT）
官	国関係機関	内閣官房内閣サイバーセキュリティセンター（NISC）、情報処理推進機構（IPA）
	自治体	大阪府、大阪市
個	セキュリティコミュニティ	総関西サイバーセキュリティLT大会、OWASP Kansai、tktkセキュリティ勉強会

（順不同）40機関（平成30年10月17日発足時点）

【共同事務局】

近畿経済産業局、近畿総合通信局、一般財団法人関西情報センター（KIIS）

（参考）関西サイバーセキュリティ・ネットワーク　平成30年度取組内容（予定）

（１）関西サイバーセキュリティ・ネットワーク　キックオフフォーラム

●日時：11月12日（月）13:30～17:00
●会場：グランフロント大阪　タワーC8階会議室（C03+C04）
●参加者数：約200名
●内容：
○主催者挨拶　森 清（近畿経済産業局長）
○基調講演　大橋 秀行（近畿総合通信局長）
○特別講演
・伊東 寛（ファイア・アイ CTO、前経済産業省サイバーセキュリティ・情報化審議官、元陸上自衛隊システム防護隊隊長）
○パネルディスカッション
「サイバーセキュリティの普及と人材の発掘・育成について」
・（コーディネータ）森井 昌克（神戸大学大学院 教授）
・（パネラー）
【学】上原 哲太郎（立命館大学　教授）
申 吉浩（兵庫県立大学大学院 教授）
【産】黒田 吉広（西日本電信電話株式会社 代表取締役副社長）
吉村 宏之（パナソニック株式会社　製品セキュリティセンター 製品セキュリティ行政部 部長）
【官】奥山 剛（近畿経済産業局　地域経済部長、元内閣サイバーセキュリティセンター参事官）
○閉会挨拶　森下 俊三（一般財団法人関西情報センター会長）
○交流会（17:30～）

（２）【企業担当者向け(初級)】サイバーセキュリティ・リレー講座

●日時：11下旬～1月下旬 16:30～18:00　＜全7回＞
●会場：KIIS会議室
●参加者数：約40名
●対象者：企業でサイバーセキュリティを担当する者（初級者）
●内容：「サイバーセキュリティの専門性を高めるにあたっての心得」

日程	テーマ	講師
11/29	AIとサイバーセキュリティ	申　吉浩　氏 兵庫県立大学大学院　教授
12/3	フォレンジック技術	上原　哲太郎　氏 立命館大学　教授
12/5	暗号技術に基づくサイバーセキュリティ	五十部　孝典　氏 兵庫県立大学大学院　准教授
12/21	ネットワーク運用とそのセキュリティ対策	川橋　裕　（他名：泉　裕）　氏 和歌山大学　講師
1/10	サイバーフィジカルシステムにおけるセキュリティ	森　彰　氏 産業技術総合研究所　ソフトウェアアナリティクス研究グループ長
1/22	サイバーセキュリティマネジメント	金子　啓子　氏 大阪経済大学　准教授
1/28	無線LAN及びLPWAにおけるセキュリティ（又はマルウェア総論）及び総括	森井　昌克　氏 神戸大学大学院　教授

○受講修了証：原則全講義に参加し、一定水準以上の理解が認められる場合（各回講義後に簡単なテストを出題し理解度を確認）、事務局から受講修了証を授与する。

（３）企業経営者層向けセミナー・イベント

●日時：11月以降　※サイバーセキュリティ月間（2/1～3/18）も念頭
●内容：　①大企業経営者向け、中小企業経営者向けセミナーやイベントコラボ（経済団体・業界団体との連携）
②サイバーセキュリティ人材をテーマとした、企業経営者層との対話企画等