National center of Incident readiness and Strategy for Cybersecurity

資料３－１

サイバーセキュリティ人材の育成に関する施策間連携の取組について

平成29年8月1日

サイバーセキュリティ戦略本部　普及啓発・人材育成専門調査会

内閣サイバーセキュリティセンター（NISC）

1．これまでの取組状況について

- 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18日サイバーセキュリティ戦略本部決定）、未来投資戦略2017（平成29年6月閣議決定）において、**サイバーセキュリティ人材育成の施策間の連携強化に向けた取組を推進**することを提示。
- 第14回サイバーセキュリティ戦略本部（平成29年7月13日）において、サイバーセキュリティ戦略中間レビュー（現状の認識を踏まえた加速・強化すべき施策を取りまとめたもの）を決定。**施策間連携に関し、セキュリティ人材の不足への対応や、高度人材の確保に向けた取組の推進**などの方針を提示。
- 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（平成29年6月26日に第1回会合を開催）を通じ、これらの方針を具体化することとしており、今後、各施策間の連携策の検討やモデル・カリキュラムの策定を行う予定。

〇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18日サイバーセキュリティ戦略本部）

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

〇未来投資戦略2017

「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18 日サイバーセキュリティ戦略本部決定）に基づき、重要インフラ・産業基盤等の中核人材育成、官公庁及び重要インフラ事業者等を対象とした実践的演習、若年層の発掘・育成等の各種人材育成施策を、各施策間の連携強化を図りつつ推進する。

〇２０２０年及びその後を見据えたサイバーセキュリティの在り方について
－サイバーセキュリティ戦略中間レビュー－

○　サイバーセキュリティ人材の不足（現在28.1万人、13.2万人不足）に対応するため、IT人材（現在92万人）が、その一つの役割としてセキュリティを担えるよう、モデル・カリキュラムの策定等必要な取組の明確化を図る。

○　関係省庁において、高度なサイバーセキュリティの技術を持つ人材のコミュニティの形成に資するよう、高度人材の確保に向けた取組を推進するとともに、各施策間の連携を図る。

【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】

・設置

第6回普及啓発・人材育成専門調査会（3/10）の決定に基づき設置

・目的

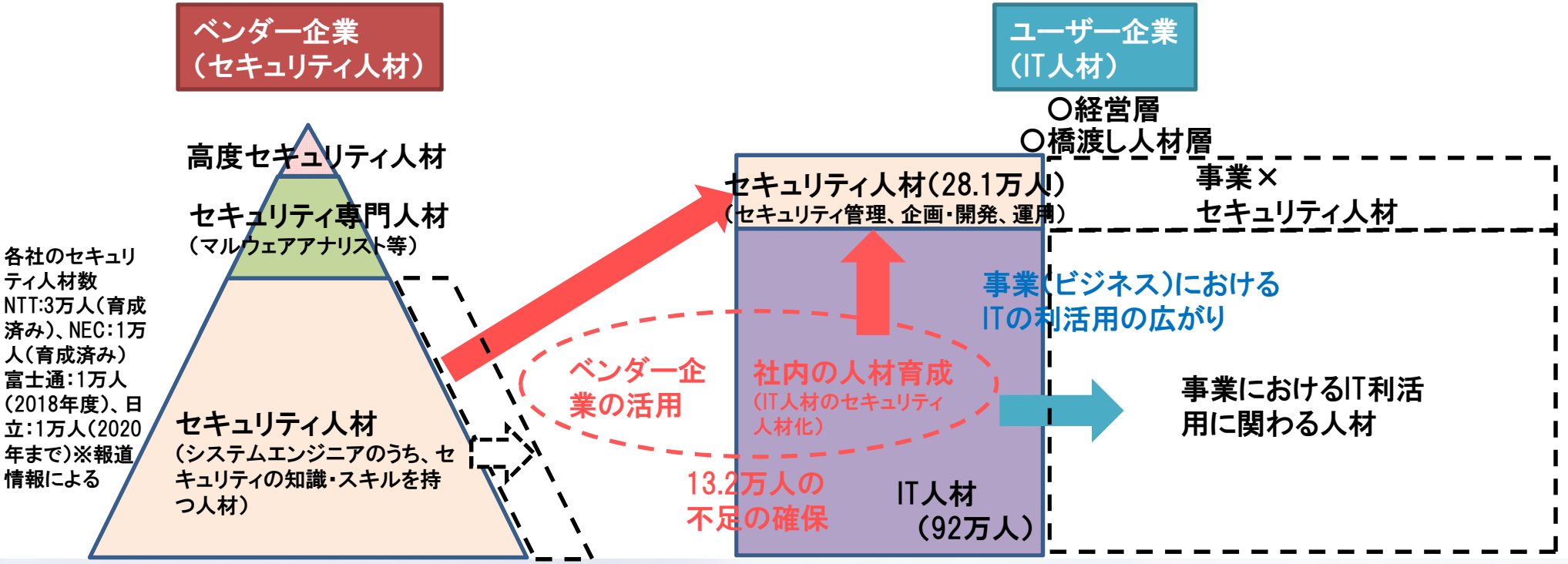
サイバーセキュリティ人材の育成に関する具体的な施策間の連携策やカリキュラムの在り方等について調査検討を行う。

・委員（敬称略）

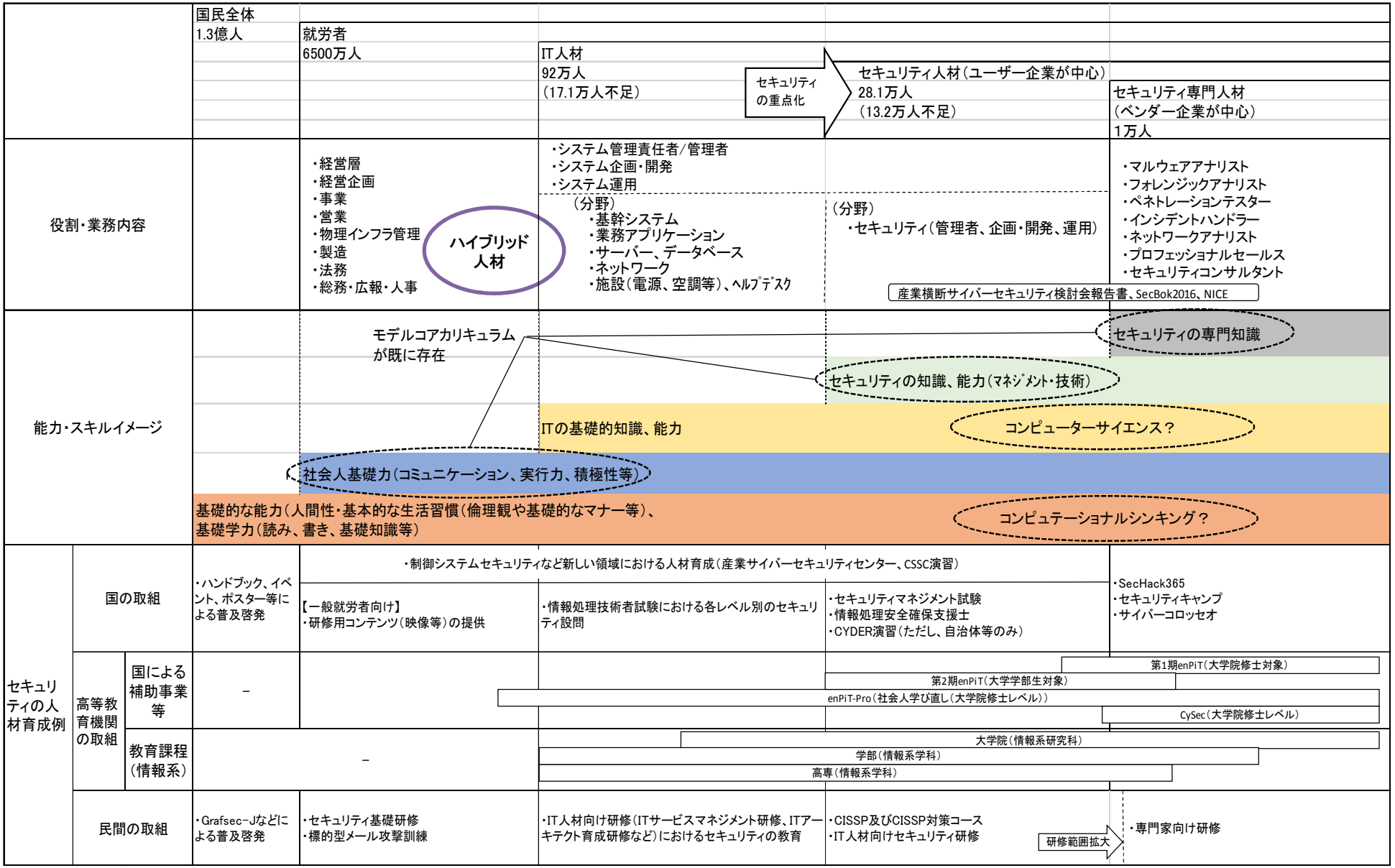
衛藤　将史（国立研究開発法人　情報通信研究機構）
川村　亨（産業横断ｻｲﾊﾞｰｾｷｭﾘﾃｨ人材育成検討会）
岸本　誠一（高知工業高等専門学校）
後藤　厚宏（情報セキュリティ大学院大学）
曽根　秀昭（東北大学）
田口　聡（独立行政法人　情報処理推進機構）

2．セキュリティ人材の不足への対応に係る論点

- ユーザー企業におけるセキュリティ人材の不足（１３．２万人）は、社内のIT人材向けの研修機会（学び直し）の創出や、ベンダー企業の活用（アウトソース）によって確保できるのではないか？
- カリキュラムに基づく教育コンテンツを最新のものにするための方策が必要ではないか？
- 学び直しのための具体的なカリキュラムとして、文部科学省委託事業（情報セキュリティ人材育成に関する調査研究）の３．３．８～３．３．１０が参考となるのではないか？
- その上で、今後、事業において情報通信技術（IT）の利活用が広がっていく中で、事業に関わるセキュリティ人材の人材像とカリキュラムを定義すべきではないか？
- 上記のセキュリティ人材育成の前提となるスキル（例えば、コンピューターサイエンスやコンピュテーショナルシンキング）とそのためのカリキュラムはどのようなものか？



（参考）役割・業務内容－能力・スキルイメージ－セキュリティ人材育成の全体像（イメージ）



3．高度人材の確保に向けた取組の推進（施策間連携）に係る論点

- サイバー攻撃の防御技術の開発や、脆弱性テスト・ペネトレーションテストによるシステムの堅牢化等を目的として、高度人材（いわゆるホワイトハッカー）の確保が必要。
- 各省庁や民間団体が、さまざまな高度人材育成の場を提供している一方、例えば、高度人材の需要の明確化、高度人材の範となるべき人材の確保、モラル教育の充実、国内CTFなど切磋琢磨できる場の創出、ビジネスへの理解など、高度人材の確保に係る各施策に共通するさまざまな課題が存在。
- 高度人材の確保に関わる国内のリソースは限られていることから、課題を整理し、施策間の連携を推進すべきではないか？

【高度人材の確保に向けた取組の例】

	SecHack365 (NICT)	ｾｷｭﾘﾃｨｷｬﾝﾌﾟ (IPA)	SECCON (JNSA)	CODEBLUE
目的	高度な技術力を持ち、自ら新たな製品等を開発していくことが出来るセキュリティ研究者や開発者を育成。	セキュリティに関する技術・知識の習得やコミュニティの形成を通じ、次世代を担う人材を発掘・育成。	実践的情報セキュリティ人材の発掘、育成、技術の実践の場を提供。	各国の優れた研究者を招聘・発掘し、国や言語の垣根を越えた情報交換・交流の機会を提供。
対象・期間	25歳以下の学生や若手社会人40名程度、約10カ月間	全国大会（80名程度、5日間）、地方大会（全国10か所程度、各100名程度、2-3日間）を開催。25歳以下が中心。	特に指定なし（若年層中心）。地方大会（1日）・決勝大会（2日間）・オンライン予選（2日間）など	特に指定なし。トレーニング（2日間）、カンファレンス・コンテスト（2日間）
内容	最先端のセキュリティ技術の研究開発体験（ハッカソン/アイデアソン）、遠隔開発実習、最先端の研究データの活用、研究者・技術者等との交流など	情報セキュリティに関する全体講義（座学を中心とした基礎的な講義や倫理観の形成を目的とした講義）と専門講義（少人数で実施する演習を交えた講義）を実施	情報セキュリティ技術を競う大会（CTF）を実施。オンライン予選・決勝大会、初心者・女性向けCTFなどがある。（いずれも基本的には年1回の開催）	各国の情報セキュリティ専門家による講演（研究成果の発表等）、実技を競うコンテスト（無料、複数種有り）、講師によるトレーニング（実習、複数コース開設）

4．今後の人材育成施策の検討スケジュール（イメージ）