資料４

サイバーセキュリティ人材の育成に関する施策間連携ワーキンググループにおける今後の検討の方向性について

平成29年6月26日

内閣サイバーセキュリティセンター

１．目的：

(1)具体的な人材像（サイバーセキュリティ人材の量・質）の基本的な認識の共有と、モデルとなる具体的な人材育成のカリキュラムの策定

(2)具体的な施策間連携の推進

（例）

－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

２．進め方：

○各機関における施策や取組の内容（具体的な教育・演習プログラムや試験制度等）やカリキュラム等について情報共有を行った上で、

(1)サイバーセキュリティ人材育成プログラムで示した課題を踏まえた人材育成のモデルカリキュラムの策定を行う。

(2)具体的な協力の項目を提示し、施策や取組の実施主体同士の連携に向けた検討を促す。

また、検討の状況については、適時、普及啓発・人材育成専門調査会に報告を行なう。

○WGの開催時期（イメージ）

第１回（６月）　：各施策や取組の共有と、今後の検討方針について提示

第２回（９月）　：モデルカリキュラム（大枠）、連携項目案の提示

第３回（１２月）：具体的な施策間連携に関する中間とりまとめ

※必要に応じて外部の有識者のヒアリングを行なうことがある。

○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

具体的な人材像（サイバーセキュリティ人材の量・質）の基本的な認識について

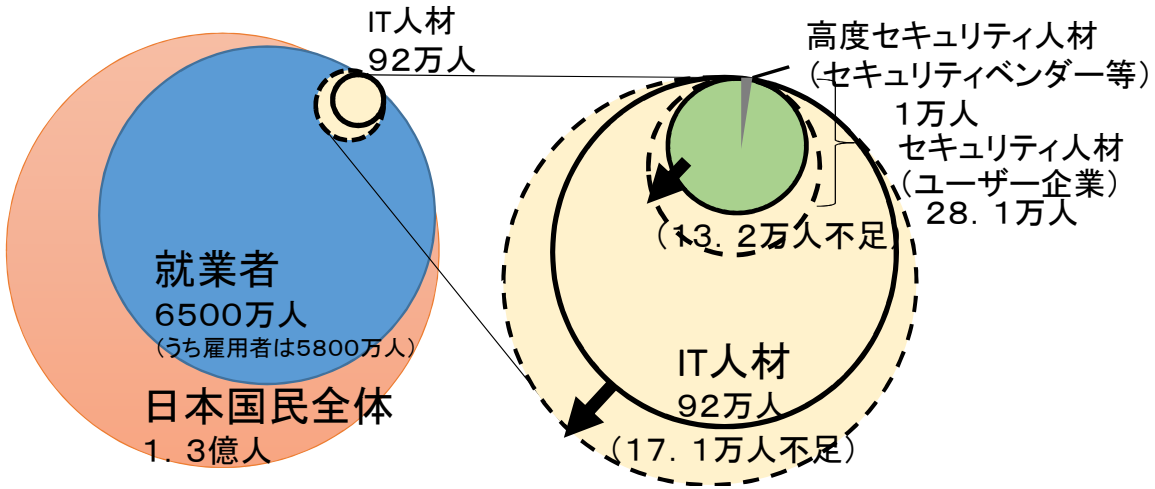
○**サイバーセキュリティ人材は、情報システムの開発・管理・利用等に関わるそれぞれの役割において、必要なサイバーセキュリティの知識と能力を身に付けた人材であること。**
→サイバーセキュリティ人材の全てがいわゆるホワイトハッカーである必要はない（自組織の防護をミッションとする人材は、チームで仕事）

○**ユーザー企業の情報システム部門などのサイバーセキュリティ人材（現在２８．１万人、１３．２万人不足）は、情報通信技術（IT）に関する基礎的な知識や能力が求められること。**
→ボリュームゾーンのセキュリティ人材は、セキュリティの専門人材ではなく、IT人材の一つの役割としてセキュリティを担う人材をさす
→ITに関する基礎的な知識・能力があれば、数週間～数か月で必要な知識は身に付けられ、あとはOJTによって育成できるのではないか

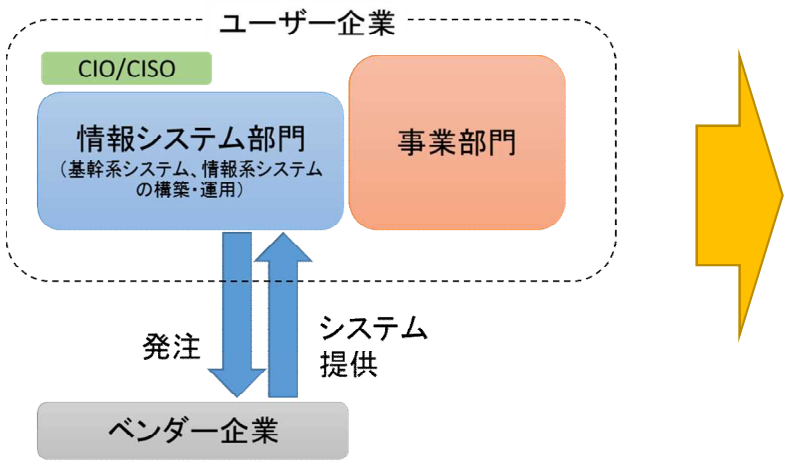
○**サイバーセキュリティ人材の育成（教育）は、官民で取り組むこと。**
→ボリュームゾーンに関しては、既に民間の研修プログラムや、多様な教材が用意されており、学ぶ機会は豊富。研修を受けさせるかどうかの経営層の判断の問題
→国が実施しているのは、民間では育成が難しい極めて高度な人材や制御系のセキュリティ人材、官公庁・自治体等のセキュリティ人材であり、それ以外は民間の人材育成ビジネスの競争の下、行われている。

○**企業等社会で活躍できるサイバーセキュリティ人材は、サイバーセキュリティの知識と能力以前に、基礎的な能力（人間性・基本的な生活習慣（倫理観や基礎的なマナー等）、社会人基礎力（コミュニケーション、実行力等）、基礎学力（読み、書き、基礎知識等））を求められること。**
→ハッキング技術だけを身に付けたホワイトハッカーは、極めて高度でない限り、社会で活躍できる幅は極めて狭い

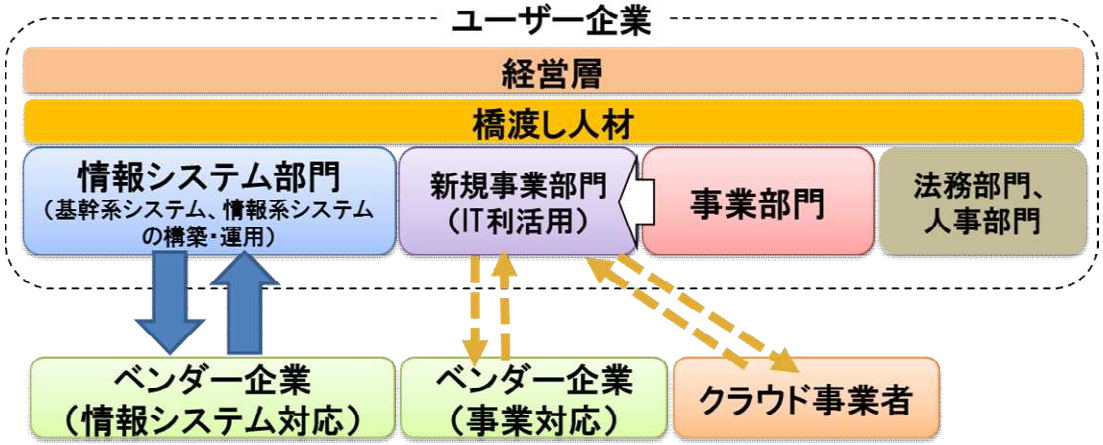
【セキュリティ人材の規模（イメージ）】



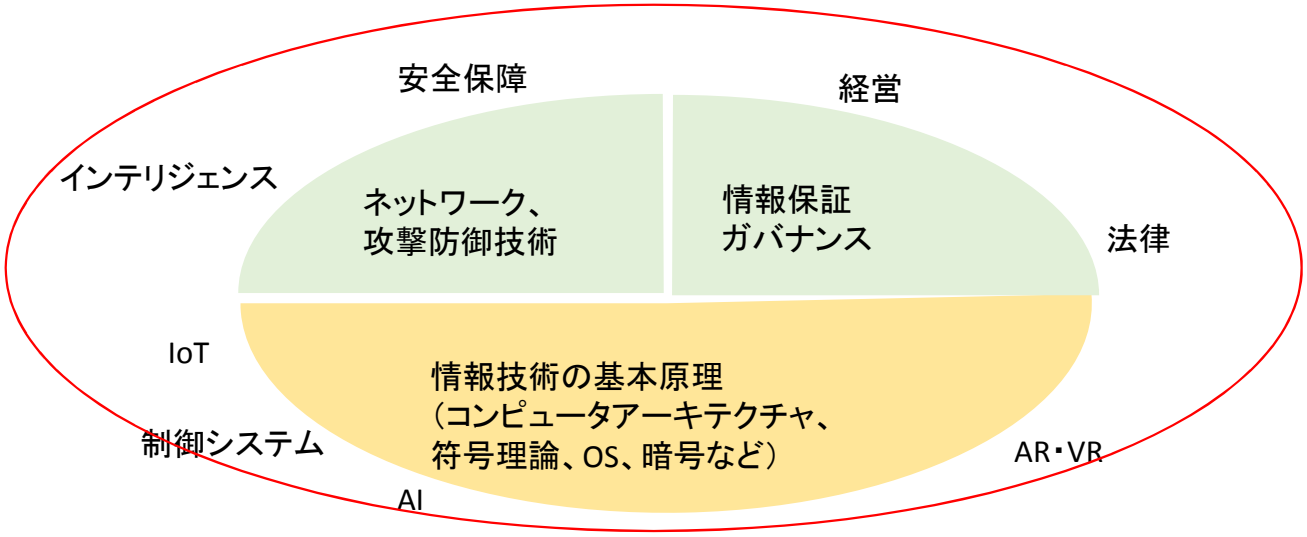
【ITの利活用により業務の効率化のための体制】



【ITの利活用により新たな価値の創造するための体制】



【セキュリティ人材に求められる知識・スキル要素の広がり（イメージ）】



【ハイブリッド人材の例】

- セキュリティ×経営
- セキュリティ×制御システム
- セキュリティ×組み込みシステム
- セキュリティ×IoT
- セキュリティ×AI

・
・
・
・

論点

- セキュリティ人材が３０年～４０年にわたって社会で活躍できることを前提として、人材育成を考えるべきではないか？
- そのためには、セキュリティに関する表層的な知識やスキルを積み重ねるような人材育成は避けるべきではないか？（表計算ソフトの使い方を習うように、セキュリティの知識や能力を高めたとしても、それだけで、生涯、社会で活躍するために必要な知識や能力にはならないのではないか？）
- 高度なセキュリティの専門性を追求するほど、情報技術の基本原理など、基礎が重要になってくるのではないか？
- むしろ、基礎的な能力や基礎学力、社会人基礎力、ITの基礎的知識や能力に立脚し、セキュリティ人材の育成は行われるべきではないか？
- 組織における実践力の高い（例えば、組織の業務とセキュリティの関係性を理解し、説明が出来ること）セキュリティ人材が必要ではないか？
- 国が行う人材育成においても、組織における実践力を考慮した取組が必要ではないか？
- IT人材がセキュリティを学ぶ際のハードル（教材やツール）は下がっており、学びやすい環境は整いつつあるのではないか？
- そのためには、

  ー役割・業務内容とモデルとなるカリキュラム、さらには考えられるアプローチを体系的に整理すべきではないか

  ー民間における取組も踏まえ、具体的な施策間連携をどのように進めるべきか？