資料１

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
第４回会合　議事概要

１　日時
平成 28 年 12 月 7 日（水）　9：30～11：30

２　場所
内閣府庁舎別館９階会議室

３　出席者（敬称略）

（会長）	安田 浩	東京電機大学 学長
（委員）	鵜飼 裕司	株式会社ＦＦＲＩ 代表取締役社長
	小泉 力一	尚美学園大学大学院 教授
	下村 正洋	株式会社ディアイティ 取締役会長、特定非営利活動法人日本ネットワークセキュリティ協会 事務局長、特定非営利活動法人日本セキュリティ監査協会 理事、セキュリティ対策推進協議会 代表
	中谷 日出	日本放送協会 解説委員
	野口 健太郎	独立行政法人国立高等専門学校機構 本部事務局教育研究調査室 教授
	浜田 達夫	一般社団法人日本情報システム・ユーザー協会 参与
	藤本 正代	富士ゼロックス株式会社 パートナー
	三輪 信雄	S&J 株式会社 代表取締役社長
（有識者）	高取 芳宏	オリック東京法律事務所・外国法共同事業 訴訟部代表パートナー（日本・米国ニューヨーク州登録） 弁護士
（事務局）	中島 明彦	内閣サイバーセキュリティセンター長
	永井 達也	内閣審議官
	三角 育生	内閣審議官
	山内 智生	内閣参事官
	阿蘇 隆之	内閣参事官
	佐々木 良一	サイバーセキュリティ補佐官
	徳田 英幸	サイバーセキュリティ補佐官

八剱 洋一郎　　情報セキュリティ指導専門官

（オブザーバー）産業横断サイバーセキュリティ人材育成検討会
内閣府
警察庁
総務省
外務省
文部科学省
経済産業省
防衛省

４ 議事概要

（１）データで探るユーザー企業のIT動向
浜田委員より資料２に沿って説明。

（２）サイバーセキュリティと法務
高取弁護士より資料３に沿って説明。

（３）企業のサイバーセキュリティに関するNISCの調査結果（速報）について
事務局より資料４に沿って説明。

（４）次期人材育成プログラムについて
事務局より資料５に沿って説明。

その後、委員による自由討議が行われた。

委員からの発言の概要は以下のとおり。

○（鵜飼委員）
資料５の５ページと６ページの「セキュリティ技術のイノベーション」には、将来的にイノベーションを生み出していくという視点と、イノベーションによって守り方が変化しても柔軟に対応できる人材の確保、という２つの視点で、整理が必要。

○（小泉委員）
初等中等教育では、子供たちが、セキュリティのマインドやスキルを獲得するために、前提となるモチベーションを持たせていくことが必要だと考えている。

○（下村委員）
セキュリティには法律系人材をはじめ様々な人材が必要になる。自社で人材を賄えない場合のアウトソースを含めて、社会として、このような人材をどのように供給するかが課題となるのではないか。

○（中谷委員）
セキュリティに明るい法律系人材を対象とした教育プログラムを開発するという視点も必要なのではないか。また、情報セキュリティの人材育成に対して世間の注目が、もう少し必要であると思う。本日、セキュリティに明るいことが弁護士業界で新たなビジネスになり得るとのお話を伺った。国としても、セキュリティが新たなビジネスモデルを創出するものになる旨を、もっと発信する必要があるのではないか。

○（野口委員）
資料５の２ページと４ページ目で、情報システム部門、新規事業部門、法務や人事部門とベンダー企業の関係が枠組みとして整理されている。中小企業を考えた場合、同じ枠組みでも、一人で幾つもの仕事をすることになる。結果として、大企業向けや中小企業向けなどで人材育成の施策を分けて考える必要が出てくるのではないか。また、教育の観点で見た場合、このような枠組みで企業が必要とする人材像と、キャリアパスの整理が必要ではないか。

○（浜田委員）
資料５の３ページの「チーム」でのセキュリティの推進は、先進的な取組を行っている企業の現状をうまく捉えていると思う。IoT の登場で IT の活用が大きく広がり、サービスや商品開発の現場がセキュリティに直結するようになってきた。こうした新しい現場のセキュリティ人材をどうやって育成していくかが今後の課題になると思う。

○（藤本委員）
これまでの情報システム部門では、IT を利用するユーザー部門のリクエストに応える仕事が中心的であった。しかし、安全性確保のための役割が重要になり、今はアウトソースする際のセキュリティやサービスを見極める目利き力が必要になっている。また、IoT などの新しい事業を開拓する場合、ビジネスに沿ったセキュリティの企画力はもちろん、既存の情報システム部門とユーザー部門との間でのコミュニケーション力、課題認識力が重要になる。

○（三輪委員）

セキュリティ対策における役割を、セキュリティの対策立案者、インシデント対応者、経営層との橋渡し役とすると、対策立案者と橋渡し役は同一人物になると思っている。このような橋渡し人材は、セキュリティ対策の大きな方針や優先順位、予算などを立案する人材であり、かつ、セキュリティと経営的な視点の双方を持つ必要がある。この点をぶれないように橋渡し人材について定義することが重要と思う。

○（佐々木サイバーセキュリティ補佐官）
インシデント対応者は、大学の演習で育てられるようになると思う。一方で、橋渡し人材の育て方は、今後の議論が必要だと思う。

○（徳田サイバーセキュリティ補佐官）
米国ではコンピュテーショナルシンキングといわれる思考方法を、教育に導入している。米国では、様々な分野の人に教育している事例があるので、参考になるではないかと思う。

○（産業横断サイバーセキュリティ人材育成検討会）
対策立案者と橋渡し人材が同一人物との意見は、その通りと思う。しかし、その両方を１人で行うのは難しいのではないかと思う。ある程度の規模の企業になると、チームでの対応が必要になるのではないか。

○（高取弁護士）
橋渡し人材の議論では、企業規模によって千差万別になると思うが、どのような権限と義務を持っていて、何か起きたときに誰にどのような責任があるのかを明確化することが重要になる。

以上