経済産業省
Ministry of Economy, Trade and Industry

産業構造審議会 商務流通情報分科会 情報経済小委員会 IT人材ワーキンググループ（第5回）-議事要旨

日時：平成27年8月4日（火曜日）10時00分～11時00分
場所：経済産業省本館17階第1共用会議室

出席委員

有賀委員（座長）、岩丸委員、佐藤委員、辻田委員、暉委員、冨田委員、西野委員、三谷委員

議題

1. セキュリティ人材の能力評価を巡る現状と課題
2. 討議

議事概要

以下、委員等からの主な意見

- セキュリティ人材とは、IT人材の中でも今非常に需要が高い、また、増やす、ないし質を高めることが重要になっているかと思う。海外の状況と国内の状況をある程度整理しておいたほうがいい。
- アメリカの場合、個人情報の漏えいとかが起きたときに、データセンターの管理者の中にCISSPとかGIACといった資格をもっていない人が含まれていた場合に損害賠償額が2桁とか3桁上がるという事情がある。
- CISSPにしてもGIACにしても、維持費が高い。情報処理技術者試験というのは基本的に個人がみずから受けるもの、資格を得るものという整理がされていると思うが、海外の場合、雇用主が資格維持を負担している制度になっている。今後、セキュリティに関する資格をある程度重要視するのであれば、個人ではなくて雇用主がある程度負担する試験制度にしていかないと、なかなか難しいのではないかと思う。
- 海外の場合、特にアメリカの場合、資格をもっている以外にも要件があって、身辺調査を大分している。本当にセキュリティを固めたいのであれば、資格をもっているだけでは不十分で、身辺調査を含めてやらなければいけない。
- ヨーロッパの場合、いわゆるホワイトハッカーに対しての倫理資格が発達している。守る技術だけ育てても余りうまくいかなくて、攻める側の技術も育てなければいけない。ただ、攻める人たちの倫理観をどう育てるのかというところを考えていかなければいけない。
- 最大の課題は、資格とか人の数ではなくて組織が能力を担保できているかということに尽きる。幾ら何人の資格者がいるといっても、実際にそれが担保されていないと意味がないということが非常に大きな課題。
- 自分たちで認識できない、気づいていない攻撃にどう対処するのかという、今まで我々が経験したことがないことをやっていかなければいけないということだと思う。人と技術、それからマネジメントのプロセスがきちんと三位一体となって、そこにリーダーのきちっとしたリーダーシップとガバナンスがあるというモデルをつくることが非常に大事。
- 仮に標的型を受けたとしても、そのときにどういうリスクマネジメントをするかということをもっている組織が日本は非常に少ない。セキュリティのプロの人たちは、リスクマネジメントは決してプロではない。リスクマネジメントの高度化は非常に大事。
- 個人の能力としてどういうことが必要かということも大事だが、組織としてどういうことが必要なのかという視点はもつ必要がある。特に、政府とか公共機関は狙われやすいので、そういったところにはしっかりこういったポリシーをもって、実行できる力をもっていなければいけないと思う。
- 知識、スキルを体系化して、BOK（知識体系）をきちっとつくって、それに基づいた資格制度のレベリングも非常に大事なのではないか。
- セキュリティ人材が8万人足りないとか言われているが、今大事なのは数ではなくて、1,000人の非常に優秀な人を育てることに集中投資すべき。
- 1人のサイバー捜査官を育てるのも大事だが、組織レベルとしてどのようなcapabilityとかcapacityをもっているかが警察も非常に大事。日本の警察のヒアリングもかなりさせてもらったが、今までのフィジカルな捜査とは全く違う世界なので、この辺もきちっと参考にしていく必要がある。
- セキュリティの世界では、イスラエルは非常に投資もしているし、人材を育成している。今、実は、もう8%ぐらいのシェアがセキュリティの世界であるぐらいにセキュリティ技術大国になっている。
- NPOであるシステム監査人協会では民間資格として「公認システム監査人制度」を創設している。面接や小論文を実施しており、その結果をもとに認定を行っている。合格者について登録を行うことになるので、その後何らかの問題があったときのために「取り消し」について

もルールを定めている。一度の試験結果だけでは本当の人材の実力はわからないため、継続教育はとても重要だと認識している。それも、単なる知識のアップデートだけでは不十分。特にシステム監査人は、システム監査を実践していくことそのものが重要になる。模擬監査実習等、実践機会をつくることも協会の活動として行っている。それらの活動をポイントに換算して、一定点数を上げることを継続の条件にしている。

- IT自体がコモディティになってきて、誰でも使えるということによっていろいろなビジネスが生み出せることの裏返しとしてセキュリティというリスクも高くなっていることは事実。そういうことを踏まえて、より一般的な人材にセキュリティ教育を行い、リテラシーを上げることが必要になってくる。
- セキュリティの確保を行うためには、技術だけではなく、マネジメントそのものや、エンドユーザーのリテラシーなどは重要な要素となる。そういうことをきちんと評価するためには第三者の目線できちんとみることが必要。
- イギリスで電子政府関連の開発プロジェクトが余りうまくいかなかった時期があり、いろいろな対策がなされてきたということをお聞きしたことがある。その中で一番有効だったのは第三者による監査だったそうだ。技術も重要であるが、第三者がきちんとした観点で、局面毎にチェックするということが大きな効果につながる。
- 大学、アカデミアにいる立場からすると、セキュリティ人材の項目ができるかというと、セキュリティというのは、今、かなり実践的になっているので、ハッキングに関するデータとか何らかの情報があれば対処できるが、大学はそういうのをなかなかもっていない。要するに、実践的な情報をもっていないという状況。そういう情報を出していただかないと大学側は対応できない。
- セキュリティ人材が足りないというのは現実なのだと思うが、ただ、そもそも供給をふやすだけではなくて需要を減らすという考え方もある。今、海外のクラウド事業者は、1人の管理者で管理しているサーバーの数が1万5,000台から2万台ぐらい。彼らはシステムを非常に均質化することによって1人で管理できるサーバーの数を減らすという形で人材を確保している、要するに規模に対してなるべく少ない人数で対応できる形にすることによって、人材不足に対応しているというようにみることができる。安直に人材の供給を増やすというだけではなくて、守るべき情報システムをなるべく均質化をして、なおかつ自動化ができる形にもっていくというのも1つの考え方。
- セキュリティの人材に関して、最初からデプロイメントしておく人材とバッファリングしておく人材の2種類があり、両者のバランスをうまくとっていかなくてはいけない。人材育成の仕方も、バッファリングしておくための人材とデプロイメントするための人材で質が違う。ちゃんと分けてご議論されるといいのではないかと思う。
- （セキュリティ対策について）どこからが行政で、どこから民間かというのは、民間と独法に関してはそれほど差がないということを考えて、うまく線引きしていただければいいと思う。人材の活用に関しても行政と民間というのを厳密に分けて考える必要もないと思う。
- 中小も含めた一般企業まで易しいセキュリティを指導できる人材と、ハッカー等の対応も含めて高度なところを国としてやっていくという人材、2通り必要のような気がする。
- 私の部門では、グループに対するポリシーだとかを中心に進めているが、そういった中でグループのセキュリティガバナンスを運営する人材が足りないということで、人はいつも募集しているが、なかなか集まらないというような課題もある。
- 私の部署でセキュリティを担当している社員には情報セキュリティスペシャリストの資格をとったりとかして勉強させている。CISSPとかも検討したが、我々のようなユーザー企業がもつには非常にコストが高い資格になっている。企業のコストで取得するとしても、もう少し優しいコストでとれて、名刺にも書けて権威があるようなうまい資格というのがあると、部下のモチベーションにもつながる。ぜひ、そういったところを狙っていただけると非常にありがたい。
- 当社は国内、海外にグループ会社があり、海外も含めたセキュリティポリシーをつくっているが、日本の知識でつくったポリシーが海外の子会社に通用しないというシーンがある。そういった視点でも、試験の中にガバナンスという考えを入れていただけると非常に助かる。
- 比較的小さい会社でも維持しやすい資格・試験というのがあって、それをもっていることによって採用しやすくなるだとか、ユーザー企業からみてそういうところが担保されて、小さいベンダーさんも担保されるというのは非常にメリットがある。資格をとっていただくモチベーションとして、比較的小さい企業に定着するといい。
- （資格の更新について）余り負担にならない程度の更新にしていただけるといい。更新料に何万円かかるというような資格になるとなかなか厳しい。1回とったら、その後はオンラインとか数千円とかで、知識があることが証明さえされれば簡単に更新できるような仕組みが望ましい。
- 資格とか、こういった試験を広めるという観点で感じたこととして、資格はもっているが、活用する場面がなかなかない。そうなると、継続して次の資格をとろう、別の資格をとろうというモチベーションにつながらない。もちろんインセンティブがある事例もいろいろと提示されていたのですけれども、もう少し、これをもっていると、こんないいことがあるというのが普及するといい。政府主体というか、強制的な対策でもいいので、インセンティブを上げる対策が必要。
- 人材育成の中で、議論をどこの人材に絞るか、整理が必要。担当者人材なのかプール人材なのか、むしろ、とがった人材なのか、各企業に置く人材なのか、普通の人材なのか、そういうところもよく整理して、どこを対象にするのか、そういうところが非常に大事ではないかと思う。
- ホワイトハッカー的なところについては、ペーパー試験では無理だろう。今、試験としてやっているのは、情報セキュリティスペシャリスト試験、開発側のある程度の人材、管理者クラスになるような人材、そういうところを主たる対象としてやっている、あと、一般の職員に関しましてはITパスポート試験という中で情報セキュリティを重視した形でつくってきた。
- 登録制度を前提とするなら、少ない人数を登録するのでは仕方ない。ある程度のスキルの人材を一定量登録していかなければ制度としての意味はない。
- 登録制度は、バイネームで動くような1,000人の優秀な人材をどう育成するかということとは別のところで考えてもいい。
- 身辺調査だとか倫理の問題について、ペーパー試験の中で、今ここのところは欠けている。ペーパー試験という中で、どうやってそこを担保できるかというところは、とても難しい話。実際に認定するとき、どのような人たちをどういう形で認定するのか、議論のあるところではないか。

- 登録を更新していくときに、試験を受かる人よりもスキルが落ちていてはしようがない。まず、そこのところをしっかりと担保することが大切。試験に受かって、そして、スキルの積み重ねがあることが大切。
- 登録制度に対して、どういうインセンティブを与えるのか。非常に難しいところ。官公庁における調達要件として、情報処理技術者試験、それから情報セキュリティスペシャリスト試験の活用、このようなことが具体的に書き込まれているが、「必置」の要件ではなく、「望ましい」要件という記述であるものの、政府の中では定着してきているのではないかと思っている。次は、政府では使っているので、民間でもいかがですかというようなところかもしれないという気もする。

今後、セキュリティ人材の実践的な能力を客観的かつ継続的に保証できるような制度の検討を行うための研究会を設置し、専門的な議論を行うこととなった。

以上

関連リンク

IT人材ワーキンググループの開催状況

お問合せ先

商務情報政策局 情報処理振興課

最終更新日：2015年8月26日