2014年4月に「サイバーセキュリティ戦略本部」を設立 サイバーセキュリティ人材育成の一環としてCISSPホルダー増員の方針を打ち出す

日本電気株式会社

日本電気株式会社（NEC）は、官公庁や企業などにおけるサイバー攻撃対策の導入・運用を支援するための体制を強化することを2012年11月下旬に発表しました。

同社のナショナルセキュリティ・ソリューション事業部 主席技術主幹であり、サイバーセキュリティ戦略本部 主席技術主幹でもある則房雅也氏とサイバーセキュリティ戦略本部 エキスパートの後藤淳氏にサイバーセキュリティ戦略本部設置の背景、CISSP導入の目的や今後の取得者増員計画などについて伺いました。

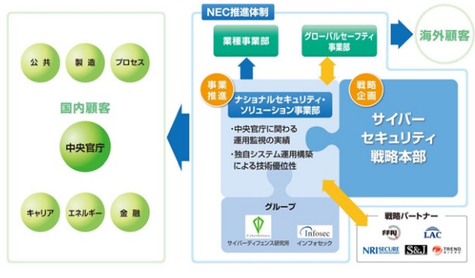
Q 御社の事業背景、情報セキュリティ部門立ち上げの背景についてお話しください。

則房　当社ではインターネットが利用できるようになった1990年以降、情報セキュリティを重要課題とし取り組んできました。私などは創世記メンバーの一人で、ファイアーウォール技術開発や構築などのセキュリティから始め、今日のサイバーセキュリティ課題に至るまで、長期間にわたり取り組みを積み重ねて参りました。

個人情報漏洩問題が世間で注目浴びたことを契機にセキュリティ強化の気運が一気に盛り上がった時期もありました。しかし、どちらかといえば、日本市場では総じてセキュリティよりも利便性を求める傾向が強く、またウェブを中心としたネット利用への取り組みが主流だったといえるでしょう。

サイバーセキュリティ事業の推進体制

サイバーセキュリティ事業のNEC全社戦略に従い、各事業部門を支援するサイバーセキュリティ戦略本部と連携し、ナショナルセキュリティ・ソリューション事業部が事業を推進



その後、個人情報漏洩について法制化されると、インターネットを利用する多くの企業が、利便性を犠牲にし、情報セキュリティに関して徹底して取り組みました。これが一段落し問題が減ると、今度は情報セキュリティ管理の効率化、コスト削減、省コスト化に取り組むことになり、結果的にこれがセキュリティ人材の離散を生むこととなりました。

ところが、2010年に防衛関連企業が大規模なサイバー攻撃を受けた事件を契機に潮目が変わり、「これからはサイバーセキュリティに対応しなくてはならない」との危機感が日本全体に広がり、当社ではセキュリティ人材を集め、サイバーセキュリティへの取り組みを本格的に始めることになりました。

まず、私が所属するナショナルセキュリティ・ソリューション事業部で国家安全保障にかかわるサイバーセキュリティへの取り組みを始めました。しかし、サイバー攻撃は国家安全保障に限らず、企業をはじめ、いかなる組織にとっても身に迫る重要な問題との認識から、サイバーセキュリティを全社横断的に担当する、「サイバーセキュリティ戦略本部」が新設され、私と後藤はここでサイバーセキュリティ戦略立案に携わっています。

この戦略立案の中で、かつて情報セキュリティに携わった人材は大勢いたのに離散している現実、「サイバーセキュリティ」には多様な知識と経験が複合的に必要となること、新しい知識や技術も必要とし、これらが大きく不足しているという事実が明確にされたのです。サイバー攻撃者は訓練され、高度な技術を保有しているため、攻撃に対応するには、より多くの人材の確保、育成はもちろん、攻撃者に劣らない技術を保有した人材への育成も不可欠で、どの企業もこれまで経験したことがないような人材育成に取り組まなければならないわけです。この事実がようやく社内で認識されました。

Q CISSPについてお聞きします。まずはその出会い、契機からお話しください。

則房　私は1989年から9.11テロを経て2002年まで米国で仕事をしていました。90年代後半からでしょうか、セキュリティ・カンファレンスに参加してみると、ほとんどのCEOやCTOが、「CISSP」を肩書きに登壇しスピーチしていました。

20年近く前のことで私も若く、単純に「格好いいな、私もいつか取得して名刺にCISSPと書こう」と思いました。2000年頃、帰国する話があり、米国でずっとセキュリティに携わった成果の一つとして、CISSPを取得することを決めました。周囲に保有者もおらず参考書もないころなので、時間をかけて独学で資格取得に至りました。

帰国後、自分の周囲にCISSP取得者を増やしたいと考えましたが、セキュリティはコストという見方が強く、なかなか積極的な人材育成は進められませんでした。話がしやすくなったのは、個人情報漏えいの法制化で情報セキュリティへの機運が高まってからで、それでも限られた技術範囲になるため、CISSP保有者の大幅増加への取り組みには至りませんでした。サイバーセキュリティになってようやく、幅広い知識、経験が不可欠となり、これを示せるCISSP保有者の大幅増加が認知されたと言えます。

後藤　私の場合は、「CISSP」なるものが自分の上司（当時は則房氏）の名刺に記載されていることに気づいたことが始まりでした。私は海外ベンダーと取引に関わっていたため、海外からの訪問者と名刺交換すると、CISSPを取得している人が少なからずいました。海外ではCISSPをセキュリティ関連のCTOだけでなく、会社を代表するビジネス開拓担当やマーケッタなら当然のように保有している資格だ、ということが次第に分かってきました。

ある日、則房から、「CISSPを取得してみないか」と書籍（※写真）を渡されました。この本はリレーのバトンだよ、と言われて何のことだろう、と思ったのですが、後日、CISSPを取得して次の人に本を渡せ、と言われていることに気づきました。結構なプレッシャーで、踏ん切りがつくまではしばらく時間がかかりましたが、CISSP10ドメインレビューセミナーを受講することができ、同月内に資格試験を受験しました。

Q CISSPを取得して感じるメリットは？

則房　海外のキーマンと名刺交換をした際に、名刺に「CISSP」と記載してあれば、お互いの情報セキュリティに関しての知識や経験の確認の時間を要せずに会話が始まり、お互いを探る時間を無駄に使わないで済みます。海外の人脈をつくり、ビジネスを展開する手として、「CISSP」を名刺に印刷しておくべきです。後藤と一緒に仕事をしていたときは海外の人と一緒に会う機会が多く、一人で会ったときでもスムーズに会話に入れるようにCISSPの取得を勧めました。

後藤　当時、まだ社内にはCISSPホルダーは非常に少なかったので、そういう意味では目立ちましたし、希少価値

「NECプロフェッショナル認定制度」の公的資格リストにCISSPを採用 専門人材不足が危惧されるなか、CISSPの存在感は高まる

を感じました。社外のベンダーとのお付き合いでも互いにCISSPホルダーだと会話も弾みました。CISSPつながりで対外的な交流も促進されます。

数年前からグローバルの認知が先行し、日本国内においても、CISSPに対する認知や価値視する傾向が強まったように思えます。

則房　海外でビジネスプレゼンや講演する際に、最初に表示するスライドに氏名とともにCISSPの記載があるか否かでかなり参加者の聞く姿勢が変わります。

セキュリティに精通しているスピーカーなのか、日本のどこか素性の定かでないビジネスパーソンなのか、という印象には大きな差が出るでしょう。英語が十分ではない日本人にとって、「CISSP」の一語だけで良い先入観を与えられるのは有益なことです。

Q 御社のCISSP資格推進に対するお考えをお聞かせください。

則房　サイバーセキュリティ戦略本部設置のタイミングで、社内のサイバーセキュリティ人材の育成を積極的に活性化させようとの方向性が示されました。現在は、サイバーセキュリティ戦略本部の取り組みの一つとしてCISSPホルダー増員の方針を打ち出しています。

現在は5日間のCISSP10ドメインセミナー受講が一番効率的なので、予算をそれなりに確保し、時間の取れる者には基本的に受講を促しています。

当社は「NECプロフェッショナル認定制度」を設けています。アドバンストテクノロジストを社内で認定する制度です。課長試験のようなプロセスがあり、かなりの難関で、その条件として公的資格取得を挙げています。

情報セキュリティに従事する者は専門職の位置付けのみで公的資格を取得していないケースも少なくないため、CISSPの取得を勧めています。同制度の公的資格リストにCISSPも採用されており、二つの公的資格取得を条件とし、CISSPはその一つとしてカウントされます。

後藤　社内資格は人事制度に組み込まれていますし、資格取得の有無は人事考課に反映される仕組みになっていますのでCISSPホルダー増員にもつながると思います。セキュリティは一人で行うよりも、コミュニティを形成し、相互に切磋琢磨することが肝要だと思いますが、当社グループ、関係するパートナー会社と共同でコミュニティ形成を目指す動きもあります。

Q 御社における人材育成の今後の展望、求めている人材についてお聞かせください。

則房　内閣官房でもリスクやサイバーセキュリティに関する戦略が立案され、法制化されました。戦略を実行するためには多種多様な事柄を実施しなければならないのですが、最大のネックはサイバーセキュリティの人材が決定的に不足していることです。最近も関係者が集まるセミナーで私が講演した際に、サイバーセキュリティ人材の育成をどうするのか、この命題は企業だけでなく大学も含め政府の先導で取り組まなければならないと主張しました。

かかる課題はセミナー参加者の反応の見る限りかなり理解され、浸透されてきているとみています。人材育成に対してどのように取り組まなければならないのか、真剣に向き合おうとしています。しかし、もっぱらの課題は具体的にはどのように取り組めばよいのか、ということです。

CISSP取得のリレーのバトンとなった書籍

サイバーセキュリティ人材が広く普遍的な価値観で認知され、その認知に基づいたキャリアパスのモデルを創出し、構築しなければなりません。このような普遍的な認知という点で今後ますますCISSPの存在感が高まるのではないでしょうか。人材育成をテーマに多様な人材が集い、ワーキンググループを形成している場においてもCISSPのニーズが高まってきていると肌で感じます。

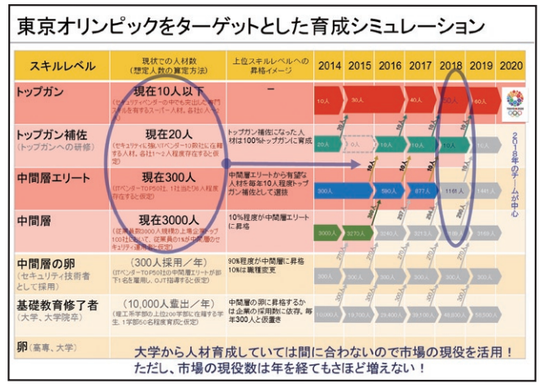
CISSPの仕組みとして秀逸なのは、専門的な知識を座学で習得するだけでなく、実際のセキュリティ現場での経験がなければ資格を取得できないというところです。また、資格継続ポイント取得により技術力を維持していかないとCISSPホルダーであり続けることはできません。

サイバーセキュリティの分野では、幅広い知識を有し、理屈が分かったうえで、実際に問題が起こったときにも対応できる技術者が求められています。セキュリティ運用管理においては、何が起こるか予想し難いので、技術者として判断できる知識とセキュリティ管理者としての判断する基準の双方を備えていることが重要なのです。技術的に掘り下げることを追及していると、技術嗜好や思い込みで判断を間違ってしまうことがあります。資格を取得する必要性を感じない人も多いのですが、CISSPホルダーになるということは、技術者と管理者のバランスを持つことにもなるので、取得を勧めたいです。サイバー犯罪でもサイバー攻撃でも、実際に問題が起きたとき現場に出向くと、このバランスが重要になります。そういう人材育成機会としてとらえてもらえればと考えています。

Q 東京オリンピックに向かうこの時期、サイバーセキュリティ人材の充実が求められていますが、懸念点はありますか？

則房　東京オリンピックまでに必要なレベルのサイバー人材確保が間に合わないと危惧しています。企業も努力するけれども大学にも政府にも真剣に取り組んでもらい、資格認定機関もトレーニングを充実させるなど、取得しやすい雰囲気づくりをしないと、結果として日本にサイバーセキュリティ人材が増えないと思います。IPA（独立行政法人情報処理推進機構）などでは国内における情報セキュリティに従事する技術者約26.5万人のうち、約16万人が質的に不足、さらに約8万人が量的に不足していると発表しています。実働可能なサイバーセキュリティ人材と厳密に見ると、桁が二つぐらい少ないのではないかと私はみています。シュミレーションした数字でみると、現時点でサイバーセキュリティ人材として、本当に攻撃された時、手を動かして効果を出せる人材は、せいぜいは3、4千人ではないでしょうか。これが日本の今の実力と認識して、早急な対応を考えるべきではないでしょうか。

米国、イスラエルなどは他国、隣国から昼夜を問わずサイバー攻撃を受けています。こういう攻撃を受けている国のサイバーセキュリティ担当者は、24時間とは言わないまでも



多くの時間、会議などで時間を取られることなく毎日いつもOJD（On the Job Development）環境に置かれています。毎日OJD環境にいるのは、守る側より攻撃者の方が充実しているはずです。この結果得られる育成効果は計り知れません。一方、日本ではサイバー攻撃を受けたときのOJD環境が作れません。サイバー攻撃に関しては、守る側が一方的に、大きなハンディーキャップを抱えます。日本はサイバー先進他国と比べて、人材育成に置いて特に不利な条件にあると言えます。単純に数字だけで考えると、守り切るのは不可能だということになります。これを克服しなければなりません。一企業の努力では不可能で、企業、大学、政府機関が協力し、海外の力も得て、いろいろなレベルのサイバーセキュリティ人材の育成に取り組まなければならないと言えます。2020年は成果を試す時、となるはずです。