知識は実践に応用して展開されてこそ CISSPは非常に体系的で実践に役立つ

NTTデータ先端技術株式会社

代表取締役社長
工学博士　CISSP
三宅 功 氏

前号の「CISSP取得推進企業インタビュー」では、NTTデータ先端技術株式会社のセキュリティ事業部セキュリティコンサルティングビジネスユニットの羽生千亜紀氏と、セキュリティソリューションビジネスユニットの植草祐則氏に、同事業部の事業展開、CISSP導入の目的や今後の取得者増加計画などについて伺いました。今号では、同社社長の三宅功氏に、経営者の視点からCISSP認定資格推進の意義、セキュリティ人材の育成などについてお聞きしました。

Q 貴社の事業背景についてお聞かせください。

当社はNTTデータの子会社で、いわゆる「IT基盤」と呼ばれる部分の設計、構築、サポートまでを一貫して行っている会社です。アプリケーション開発はNTTデータ本体が行うのですが、そういったアプリケーションを動かすハードウェア、システムソフトウェアなどを組み合わせながら最適化して、お客様に提供しています。大手の金融機関や公共機関などミッションクリティカル（24時間365日、止まらないことを要求される業務）な高難易度の案件を対応しているため、基盤もそれに対応したパフォーマンス、信頼性を保障していく必要があります。

当社は若い会社で、設立16年目（1999年8月設立）です。実質的に現在のようなビジネスに取り組み始めたのは2000年代初頭からですので、今年が15年目になりますね。オープン系の基盤というものが現時点では広がっていまして、単にサーバーやオペレーションシステムの最適化だけではなく、それを収容するデータセンターの物理的な設計も業務としています。さらに、子会社のNTTデータ・セキュリティを2011年に事業統合しています。実はセキュリティ分野も基盤構築には欠かせない条件になっています。つまり、IT基盤の電源立ち上げから、それに必要となるハードウェア、ソフトウェアの最適構成、最終的にはセキュリティ要件までをビジネスとして扱っています。

Q 貴社にはCISSP認定資格者が多くいらっしゃいます。今回、経営者自らが資格取得に至った理由をお聞かせください。

主な理由は二つあります。一つはセキュリティ事業を始めたこと、もう一つはNTTデータ先端技術という会社をマネジメントしなければならない経営者の立場からの観点です。

経営者の観点から見るとよく理解できます。セキュリティはどうしてもコストがかかる。しかし、ご承知のとおり、昨今はサイバー攻撃の問題も頻発してきていますし、セキュリティの問題を経営者としてどのように考えるべきなのかが、ここ数年、私自身の課題でもあったのです。それなら一度、ちゃんと勉強しておこうと、私自身がトライしてみたわけです。

私自身の経歴を話しますと、私はずっとR&D（研究開発）に携わってきまして、この会社に異動になったのが2003年です。その時は会社が立ち上がったばかりで社員が30人もいませんでした。それから4年ほど社長として歩み、2007年にNTTの持ち株の研究所に戻り、4年間、研究所長を務めました。実はその研究所でもセキュリティは取り組んでいましたので、セキュリティの動向に関する情報をキャッチできる機会はありました。その後、2011年にもう一度NTTデータ先端技術の社長に戻りました。

社員も少なく、会社が小規模のときは社長の私自身がしっかりと目を光らせ、気を配っていれば、セキュリティに至るまで大抵何でも把握できました。しかし、現在のように会社規模も大きくなり、社員数が500人を超えると、ビジネスに関わる協同者・パートナーも同数以上になり、千数百人規模を抱えてビジネスを回し始めるようになるわけですから、セキュリティ上も課題が出てきます。

最初に社長に就任して間もなくして、社員数が100人を超えた頃にPマークやISMSを取得しました。しかし、このような一般的な情報セキュリティの枠組みだけではどうしても限界があります。直面する課題を何とか解決しなければいけないと思い立ち、冒頭に申し上げたように、私自身が専門資格を取得する決断をしました。

実はもう一つ動機がありました。やはりセキュリティ・ビジネスの一端に関わっていますので、お客様の経営トップとも会話する機会があります。昨今の情報漏えいなどの事件をみて分かるように、結局経営者が何をすればよいのかが理解できていないのが現状です。「ISMSを取得していればよいのか」「ハッカーを雇わなければいけないのか」などと聞かれることがあるのですが、これらに対してどう答えればよいのかと思案することが問題意識を高じさせる要因になりました。

当社のセキュリティ事業部は、インシデント・レスポンスから、診断、監視などもサービスとして網羅していますので、彼らとも議論しながら、オーバーオールでの知識体系として一度学んでおかないと話ができないと感じ、資格取得を考えるようになりました。

Q 資格取得について、今後の貴社のお考えをお聞かせください？

CISSPはどちらかというと、セキュリティ・ビジネスに関わる人たちの資格として捉えられているようなのですが、今回私自身として認識できたことは、決してそうではないということです。先ほど申し上げたように、例えば、データベースの専門家、オペレーティングシステムの専門家など、当社にも多岐にわたる技術分野のメンバーが所属しています。CISSPのCBK（共通基盤知識）8ドメインの中には物理的セキュリティも含まれるなど、データセンターの設計においてもセキュリティは非常に重要なのです。セキュリティ事業部以外のメンバーでキーになる人間に対しては、可能な限り、CISSP資格を取得するようにと話し始めているところです。私自身が資格取得しましたので、掛け声だけでなく、実効的な推進力があります。

Q セキュリティ・ビジネスに直接関わっていない人たちにとっても資格の取得は有効だと？

資格を取得することで、データベース一つを例に取っても、それを運用する体制の構築から始まり、大手のお客様に対しても単純にデータベースを稼働させる観点だけではなく、どのようにセキュリティを駆使すればよいのかまでもコンサルティングすることが可能になります。われわれは設計構築の工程を請け負っているわけですが、「とにかく作って動かせばよいと短絡的になりやすく、セキュリティの要件が外れてしまいやすくなります。特に効率性を考えた場合、どうし

NTTグループとしてセキュリティ人材強化 初級クラス10,000人、ミドルクラス2,000人、トップガン100～200人を目標に

てもセキュリティの要件を見過ごすことが多くなります。ですから、設計やコンサルティングを担当するメンバーに基礎知識として資格取得を勧めていきたいと思います。

Q NTTグループとしての取り組みについてはいかがですか？

昨年（2014年）10月、当社、NTTデータ先端技術の次元だけでなく、NTTグループとしてのセキュリティ人材育成を鵜浦社長自ら発表されています。初級クラス10000人、ミドルクラス2000人、トップガン100～200人程度をNTTグループ全体として育成するとの大胆な目標が掲げられています。東京オリンピックが開催されることもあり、セキュリティ意識を高めざるを得ない環境にあるともいえます。

私自身、セキュリティ人材の育成に注力することは良いことだと思っています。NTTデータ以外の4社は通信キャリアですから、セキュリティを重要なサービスとして提供している会社です。当社もレベルの高いメンバーを対象にした研修コースを提供するなど、教育面を中心に全面的に協力したいと考えています。

Q CISSPのプログラムと他の情報セキュリティ系の資格内容の違いは？

私自身もいくつかのプログラム、例えば、大学のカリキュラムやIPA（独立行政法人 情報処理推進機構）の推進資格なども調査してみました。どのプログラムも部分的にはいいのですが、総合的に横串で知識体系を整理している点では、CISSPが最も優れています。特に大学などの教育機関でのセキュリティ教育では、どうしても暗号化や形式手法に偏ってしまいがちです。しかし、実践を考えると、ガバナンスや運用、物理的セキュリティなど実践的な知識体系なり知識の連携が必要になります。他のプログラムではそのような例はなく、CISSPは非常に体系的で実践に役立つと感じました。もちろん、知識はあくまでも知識ですから、実践に応用して実際に展開していかなければ役には立ちませんが…。

Q 貴社には CISSP認定資格者約30人おられます。実際の業務に役立つための工夫などされていましたらお聞かせください。

セキュリティ事業に関わるメンバーは、監視やコンサルティングを提供するにあたり、診断だけでなく、お客様全体のセキュリティ対策までも俯瞰した形でコメントしたり、対策案を提示したりできます。インシデント・レスポンスのチームなども同様です。ですから、実際のビジネスを展開しているメンバーの役に立っていますし、さらにそれを他の分野のメンバーにも広めていく必要があると考えています。