

# 優れた監査サービスを提供 最先端技術に対応する 第三者としての立場から

ネットワークシステムズを母体に、ネットワークに関する専門知識を駆使したセキュリティ監査・システム監査・電子認証局監査などの第三者監査・審査・認証サービスを提供する企業として設立されたビジネスアシュアランス。同社社長の山崎氏は、国のセキュリティ関連委員を歴任し、情報セキュリティに関する高い見識を持つことでも知られています。ビジネスアシュアランス設立の狙い、同社のビジネスの大きな柱である自治体の監査と課題、さらに今後の情報セキュリティ監査のビジネスの展望などについて伺いました。

## 第三者として監査の客観性を担保 情報セキュリティ監査の大手を目指す

**Q** まず御社の設立経緯と、情報セキュリティ監査のビジネスにどのような将来像を描いておられるのか、お聞かせください。

**山崎氏** ビジネスアシュアランス設立には大きく3つの理由があります。一つは、独立性の確保、次にブランディングの確立、そして人の育成、教育といった人材の問題です。

まず、独立性ですが、システムを構築するものとそのチェックを行うものが同一では、監査業務においては公平性、客観性を問われるためです。厳格な監査を実施する上で、第三者としての立場を明確にするためにも別会社であることが不可欠と考えました。

ブランディングの確立とは、監査のスペシャリストとして業界のトップ3もしくはトップ5に数えられる存在になることを目指すというものです。情報セキュリティ監査のビジネスは、立ち上がりからそれほど日が経っていませんが、いずれは他のビジネスと同様に大手トップ5程度の企業で全体の7割のシェアを占めることになるでしょう。我々がターゲットとしているのはその7割の市場であり、それを実現する技術、人材、ノウハウを持ち合わせていると自負しています。

最後の人の問題ですが、情報セキュリティ分野の技術の変遷は非常に急速で、今日の最新技術もすぐに陳腐化するという現実があります。それだけに一度、技術の現場を離れてしまうとキャッチアップが難しくなります。その点、ビジネスアシュアランスは、ネットワークシステムズという母体を持っていることが大きな強みとなります。ネットワークシステムズは、海外セキュリティ製品のベンダーやセキュリティの専門家と頻りに交流し、常に最新の技術や標準化の動向をモニターしています。一方、当社は監査業務を通じて多くのお客様のシステムに触れることができます。実際、このような経験ができるSEはほとんどいません。そこで、我々とネットワークシステムズとが

連携し、お互いの持つ情報とノウハウを共有することで、第三者として客観性を保ちつつ最先端技術の監査に対応できる優れた監査サービスをお客様に提供できると考えています。

今後の展開ですが、いずれ情報セキュリティ監査のビジネスが大手中心に集約されていくにつれ、監査の質および人材がよりクローズアップされていくと思います。そこで、地方で監査ビジネスを行っている企業や、中小の企業などに我々の技術、ノウハウを提供するなどによって提携を進めたり、さらにはM&Aを模索するなど、積極的にビジネスの拡大を進めていこうと考えています。

## 現状の自治体の監査は 非効率な面が多い

**Q** 御社では自治体の監査をビジネスの大きな柱としていますが、現在の地方自治体の状況や今後について、監査する立場からお聞かせください。

**山崎氏** 現在、ネットワークシステムズ時代を通じてこれまで多くの自治体の監査を行ってきた経験から言えば、各自治体の情報セキュリティの格差は非常に大きく、中でもリスク分析の差が見られます。実情を言えば、自治体の情報セキュリティレベルは、各自治体の担当者の知識や熱意に依存しているという側面が強いのです。しかも、3年もするとその担当者も異動してしまうため、それまで築き上げてきた手法やノウハウ、情報も多くの場合、そこで途切れてしまいます。監査についても同様のことが言えます。これは監査業務の公募方法にも問題があるのですが、今年実施した監査の成果、受けた助言が翌年の監査にうまく活かされないケースが少なくありません。

全国には約1800の自治体がありますが、どの自治体も例外なく予算の確保が難しい。自治体の情報セキュリティ監査で第一に求められるのは、できるだけコストを抑えた監査です。特に、小規模な自治体が確保できる予算で質の高い監査というのは正直言ってかなり無理があります。そのような制約の中で、コストを抑えながら効率的かつ質の良い監査を実施するには、初年

度にジェネラルな監査を実施したら、翌年はその監査結果を踏まえ、しっかりと優先順位を付けて、問題点に特化したり、より掘り下げた監査を実施しなければなりません。しかし実態は、監査計画が単年度で終わっているため、翌年も同様のジェネラルで広く浅くという監査が繰り返されるケースが数多く見られます。もちろんこれでも一定の成果は得られますが、限られた予算で最大の効率化を求めるなら、しっかりとリスク分析に基づき、何に取り組むか優先順位を付け、改善を図っていくことが必要です。これによって本当にPDCAサイクルが機能することになります。

## 自治体の監査ビジネスは有望な市場

**Q** 一般企業と自治体の監査での大きな違いは何でしょうか

**山崎氏** 自治体の業務や実情に精通したり、自治体のアプリケーション開発の経験を持つ人材が不可欠です。その点で我々の経験は大いに役立つと思いますし、他社と比較した強みと自負しています。また、自治体の担当者の方々のサポートとなるよう、自治体における監査事例をはじめ、監査に必要なコストの目安、監査業務を公募する際の仕様書の書き方など、参考となる情報を広く提供していく予定です。

自治体が扱う情報は、個人情報をはじめ厳格な取り扱いを求められます。特に個人情報の扱いは人権そのものと言っても過言ではないでしょう。人権の平等は憲法で保障されているものであるのに、その扱いが自治体ごとに異なるようでは大きな問題です。本来は、国の責任で、リーダーシップをとって全国共通の環境整備を進めるべきだと思います。特に、自治体のシステムはLGWANのネットワークを通じて全国つながっていますから、どこかの自治体に脆弱性があれば、全体のセキュリティにも大きな影響を及ぼすことになりかねません。

先ごろの住民基本台帳法の改正では、住基システムの監査について触れられ、法案に盛り込まれています。このように今後は、国策として自治体の情報セキュリティ整備が強制力を持って進められることになるでしょう。そこで当社としても、自治体の監

査ビジネスを有望な市場になると捉え、はじめに取り組むビジネスの大きな柱に位置付けています。

## 保証型監査が普及するには 実装レベルまでの具体的な基準が不可欠

**Q** 現在、保証型情報セキュリティ監査の推進に向けて、JASAも地方公共団体セキュリティ対策支援フォーラムと協同して「オーディットレディ宣言プログラム」に取り組んでいます。このプログラムをどうお考えですか。

**山崎氏** どこかの自治体が率先して保証型監査を実施すれば、それがきっかけとなって一気に拡大する可能性はあると思います。ただ、実際は保証型監査を実施するまでの水準に至っていないのが現実です。各自治体に共通する声としては、「何をどれだけ行えば良いのか分からない」というものです。つまり、自治体向けのセキュリティ・ガイドラインがあっても、例えば、「ファイアーウォールのパラメータ設定はこうです」といった実装段階にまで踏み込んだ具体的な基準はありません。そのため、どこまで対策を行えばOKとなるのか、判断できないのです。

当社は、2年前からクレジットカード業界のセキュリティ要件に関する業界統一基準 PCIDSS (Payment Card Industry Data Security Standard) の普及に取り組んでいます。この基準の根底には、サプライチェーン・リスクマネジメントという考え方があります。具体的には、カードの発行会社、加盟店、データ処理を委託されているデータセンターなど、カードの決済処理に関わるすべての過程で共通の基準でリスク管理を実施しています。もちろん実

装レベルまで具体的に基準が定められています。

国としても権限の問題もあるので、自治体の取り組みに細かく口出しするのを避けていることもあります。一方の自治体側からすると具体的な基準を決めて欲しいというのが本音なのです。自治体の業務は規模の大小はあっても、民間企業のようにまったく業務内容が違うということは無いでしょう。それだけに共通の基準も作りやすい。そして法的に自治体のデータ・セキュリティ・スタンダードが制定されれば、対応している自治体とそうでない自治体が出てきますが、対応するには何をすれば良いのか明確化できます。もし、対策を行う上で予算の問題があるなら国の補助で解決していく。それが理想であり、そうなることを個人的にも強く期待しています。こうしたアプローチがあってこそそのオーディットレディ宣言だと思います。

また、民間企業においても、業界ごとにセキュリティ・スタンダードが策定されるといった流れができて欲しいですね。

**Q** 情報セキュリティ監査の市場を盛り上げてゆくために、JASAへの期待、要望がありましたらお聞かせください。

**山崎氏** 何より市場を形成するための努力をして欲しいという点ですね。それなりの市場（ビジネス）が存在しなければ、それを目指そうという人材も集まりませんし、優れた監査人が育ちません。そして、監査の質が問われるようでは、市場が大きくなっていくことはありません。その意味からも、情報セキュリティ監査の市場が確立され、プラスのスパイラルが動くような仕組みが絶対に不可欠だと思います。



ビジネスアシュアランス株式会社  
代表取締役社長 山崎 文明 氏

### プロフィール

システム監査、ネットワークセキュリティ、セキュリティポリシーに関する専門家。大手外資系会計監査法人にてシステム監査に長年従事し、現在、ネットワークシステムズセキュリティ事業推進本部部長を務める。内閣官房安全保障危機管理室情報セキュリティ対策推進室WG委員など数多くのセキュリティ関連委員を歴任、警察政策学会正会員、日本セキュリティ・マネジメント学会正会員。システム監査技術者、米国公認情報システム監査人、BS7799スペシャリスト。