グローバル事業の展開において戦略的かつ公平な判断のできるベンダーフリーの認定資格CISSPは有効、セキュリティ専門家としてのスキルの裏付け

株式会社 日立システムズ

株式会社日立システムズは、日立グループの情報・通信システム事業における中核企業として、幅広い規模・業種にわたる業務システムの構築と、データセンターやコンタクトセンター、ネットワークなどの多彩なITインフラを生かした システム運用・監視・保守が強みのITサービス企業で、連結ベースの従業員数は17,000名を超える企業です。

同社のクラウドICTサービス事業グループ理事 主管技師長（サイバーセキュリティ）の本川祐治氏に同社の事業展開、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。

株式会社 日立システムズ
クラウドICTサービス事業グループ
理事
主管技師長（サイバーセキュリティ）
本川 祐治 氏

Q 貴社の事業の特徴、貴社におけるCISSP資格の位置づけについてお聞かせください。

日立製作所、日立グループとして情報システム関連業務を受注した場合、セキュリティ運用に関しては主に当社がサービスを提供します。セキュリティ関連製品の販売・導入などは、日立製作所や他の日立グループ各社も提供しますが、導入後の実際の運用については当社の担当領域になります。

セキュリティ関連企業の一般的な事業領域はインシデント監視サービスのみの提供、あるいは脆弱性等に関する検査実施と分析結果報告がその大半を占めるなかで、当社はその範囲にとどまりません。インシデント監視状況とインターネット上の膨大な情報から得る最新の脅威情報による総合的な分析により、信頼性の高い情報提供が可能なだけでなく、顧客企業のシステムを当社SOC（Security Operation Center）で運用する場合、検知した脅威への対策を講じることも可能です。予兆に対する迅速な対応により、被害拡大を防止します。

最近、「社会インフラ・セキュリティ」という言葉が耳目を集めています。日立グループは創業以来、「社会インフラ」に関するソリューションを提供してきましたので、「社会インフラ」に関連性が高い情報セキュリティシステムをインフラ全体の運用サイクルに融合できるように活動するのが当社の役割です。

当社は長年にわたり、「SHIELD（シールド）」というセキュリティ・ソリューションを提供しています。「SHIELD」は、顧客企業の情報資産を守るためにセキュリティ導入時のコンサルテーションからシステム構築、運用まで、セキュリティに精通したエンジニアが対応するワンストップソリューションです。

-SHIELD SOC-

従って、「SHIELD」を展開する上で、実際にかかるソリューションを担うメンバーがどのような資格を保持しているかが問われます。その資格の一つにCISSPを位置付けています。事業環境は日々変化していますが、CISSPを継続的に推進する体制は変わっていません。情報セキュリティ関連の資格として他の国際的な資格もありますが、当社としてはCISSPを標準的な資格として推奨しています。資格保持が昇格認定の一つにもなっています。

Q 貴社のグローバル事業展開に対するお考えをお聞かせください。

日本の顧客企業の世界進出、グローバル事業展開を支援することが端緒となると考えています。現在は、米国のHitachi Data Systems Corporation（日立データシステムズ／以下HDS）と協力してグローバル事業展開に取り組んでいます。HDSは、従来のストレージの開発や関連サービスの提供に加え、近年強化した運用を行ううえでセキュリティが必要になるため、当社がこの領域をグローバルの次元で担っています。つまり日立グループ各社が提供するセキュリティ分野の多くは当社が運用しているわけです。

海外において、当社が表に立って直接セキュリティサービスの営業活動することとはありません。セキュリティは、当社単独で販売できるものではないからです。各国の企業がHDSのソリューションを利用するようになり、「ストレージに対するセキュリティが必要だ」、あるいは「日立が提供したインフラシステムに対してセキュリティが必要だ」となった段階で、当社のサービスを利用する機会が訪れることになります。

Q CISSP取得者をかかえていることによる、事業上の具体的な利点は何ですか？

例えば、HDSのメンバーと商談するシーンでこのようなことがあります。彼ら自体は米国拠点のグローバル企業ですから、いよいよ商談するにあたり彼らと最初に握手するとき、「日立システムズがセキュリティを売り込みに日本からきたけれど、あなたたちはセキュリティについてどのレベルの見識を持っているのか？」と問われるわけです。このようなシーンでは、CISSP認定保持者が、CISSPのバッジを身に着け、「私たちはCISSP資格を取得しています。あなたたちと同じCISSPホルダーです」と説明すると、HDSのメンバーは「セキュリティに関する基本線を押さえており、共通知識を理解できているのだな」と彼らは認めるわけです。

海外のシステムインテグレーター系のベンダーたちとの関係においても同様です。「CISSPのホルダーが何人いて……」と説明すると、「なるほど、わかった」と前置きの話がその場で終わり、即商談に入れるのです。まず、技術レベルの詳細を問われた場合には、長々と詳らかに細部を説明するよりもCISSP のホルダーであることを表明したほうが商談は格段にスムーズに進行します。

Q CISSPのホルダーを増やすこと自体にも意味があるということですね？

その通りです。グローバルレベルでの事業展開や、各国の

現在は、技術分野以外の社会学的セキュリティと称する分野の人間もCISSPを取得が望まれる

省官庁と仕事をする場合、各国の多様な組織や団体と商談することになります。グローバルに通用するCISSP資格を保持しているか否かで、席上での展開が全く違ったものとなります。CISSPは国内外の情報セキュリティ分野に精通した人々とのつながりをカバーリングする資格だと思います。前述の通り、CISSPホルダーであると表明するだけで、「CISSPのCBK10ドメインを理解しているから、そこから会話が始められる」となるのです。

セキュリティ分野のテーマで経営層と会話したり、ある一定レベルの経営指南をしたりするビジネスパーソンにとっては、単にセキュリティのコンセプティングや診断ができるだけでは意味をなしません。現在は、セキュリティの情勢分析、つまり社会学的セキュリティと称する分野の人間もCISSPを取得しているか否かで差が開きます。組織におけるバックグラウンドも重要ですが、それだけでは通用しません。ですからCISSPの取得を推進する必要があるのです。

Q セキュリティ人材の育成に対してどのようにお考えですか？

日立グループ全体として技能向上に重点を置いています。CISSPホルダーが技術的な能力を有する人材のレベルアップを指導しています。

日本国内最大規模のセキュリティコンテスト「SECCON」（NPO法人日本ネットワークセキュリティ協会主催）に協賛することを通して、情報セキュリティの先端的なテクノロジー習得に対して支援する観点も当社は持ち合わせています。優秀な情報セキュリティ技術者の育成とスキルの高度化に取り組んでいるのです。

「運用」と言うと、とかくオペレーターがごりごりシステムをいじっているイメージを抱かれます。しかし、実際には、例えば、マルウェア解析やフォレンジックも「運用」の一つになります。

「運用」は、情報セキュリティの領域でかなり広範でかなり深い技術をもっていたとしても、例えば、単にマルウェア解析をできるだけでは通用しません。それがどのような背景で発生したのかまで考えが及ばなければなりません。なぜマルウェアが侵入したのか、動きそのものはテクノロジーだが、どのような情報を入手しようとしていたのかなど、分析が欠かせません。

当然ながら、「社会インフラ・セキュリティ」について語ろうとする場合、監視カメラなど物理的なセキュリティなど全て含まれますので、CISSPのCBK10ドメインの中の「物理セキュリティ」で学ぶ、カメラの設置に関する内容などは基本事項として非常に役立っています。かかる内容がベースとなって、カメラの設置位置やデザインに対して助言をすることも可能となるのです。

Q どのような人材の育成を目指していますか？

やはり情報セキュリティ技術、ならびにセキュリティ関連知識の網羅性を兼ね備えていないと仕事にはならないと考えています。

前述のSECCONのように深い情報技術に精通する人材育成をめざしています。確かに深い情報技術に精通する人間も必要なのですが、これらに精通した人間がさらに分析した結果をお客様のその本来あるべき業務を支援するときに、本来あるべき業務、あるいは社会インフラシステムはどうあるべきかについて推測したり、こうあるべきだと助言したりすることのできる幅広い知見、判断基準が必要なのです。

このような知見や判断基準をOJTに取り組む中で深めつつ、深めたことを確認する意味でも、CISSP資格取得でカバーしていきたいと考えています。数多の資格が存在するなか、グローバル基準で認められる資格を持ってもらいたいのです。私は世界最大のセキュリティコンテストである米国の「DEFCON CTF」に過去参加したことがあります。その観点からも若年層の技術者は先端技術の習得から始め、それを実際に運用したり、OJTに取り組んだりする中で幅広く覚え、確認し、確固たるものにするために、（ISC）2の講座を受講し、CISSP資格の取得に挑戦してほしいと考えています。