



社内技術者のスキルアップはもとより 日本のセキュリティ技術を国際レベルに引き上げる CISSPには無限の可能性を感じます

株式会社日立情報システムズ

資格取得推進のポイント

● 経営課題・ビジネス背景

2010年までの中期目標にセキュリティ分野の飛躍的成長が盛り込まれた。

● 導入目的

セキュリティ技術者における専門性の底上げとスキルを判断する評価尺度が求められた。

● 導入プロセス

CISSP10ドメイン インハウスセミナーを定期的開催し、実務経験4、5年の技術者を受講させている。

● 取得効果

CISSPを中心に配置し、「SHIELD 110番」を立ち上げることができた。

昭和34年(1959年)の設立以来、情報サービス業をコア・ビジネスとして展開されてきた株式会社日立情報システムズ様。特に最近、個人情報保護法や日本版SOX法などが施行され、情報セキュリティ対策を支援するソリューションへのニーズが急速に高まっています。こうしたビジネスチャンスを的確に捉え、市場シェアを拡大していくための施策に取り組んでおられる、セキュリティソリューション部 部長 本川 祐治氏に、CISSPの導入理由とその活用方法などについてお聞きしました。

導入目的は、社内技術者のスキル評価と日本のセキュリティ技術の底上げ

私がCISSP認定資格を導入した理由はふたつあります。ひとつは、セキュリティ技術者のスキルを客観的に評価するためです。お客様の所へ行ってコンサルティングをしたり、設計をしたりするわけですから、確かな人材でなければなりません。その人材のスキルを評価するとき、さまざまな資格がある中で、必要な知識を網羅的かつ体系的に学んだCISSP認定保持者なら、自信を持ってお客様の所へ送り出せると考えました。もうひとつは、日本のセキュリティ技術を国際レベルに引き上げたいという広い視点に立ったものです。私はセキュリ

ティシンクタンク「Black Hat」やISACA(情報システムコントロール協会)の日本コーディネーターも兼任しており、海外ミーティングにたびたび出席します。そこで痛感するのは、世界で通用するセキュリティ資格の取得率が、日本の場合極めて低いということです。このことは国外のセキュリティ技術者にもよく指摘されます。そのような意味から、ANSI(米国規格協会)よりISO/IEC17024の認証を受け、グローバルに認められているCISSP認定資格を取得することが、日本のセキュリティ技術全体の底上げになるものと考えています。

CISSP大幅増を目指して積極的にインハウスセミナーを開催し グループ内からスキルアップの輪を広げる

CISSPの導入プロセスとして、当初は実務経験4、5年のサブリーダークラスの技術者数人を (ISC)²公式CISSP10ドメインレビューセミナーに参加させて、CISSP認定資格を取得させました。その受講内容を吟味したところ、セキュリティ技術の向

上を日立グループ内から高めて行こうとする、我々の計画を実現できると確信しました。そこで、(ISC)² Japanに問い合わせたところ、参加者数により社内のセミナー会場に (ISC)²認定講師を招いて社員に受講させる、インハウスセミナーとい

CISSP認定資格が 情報セキュリティ技術者の スキルを向上させ 時代を先取りした セキュリティサービスを 創出していきます

株式会社日立情報システムズ
ネットワークサービス事業部
ネットワークシステム本部
セキュリティソリューション部
部長

本川 祐治 氏



う形態の受講も可能であることが判明しました。さっそく参加者を募って2回開催したところ、19名のCISSP認定保持者を輩出することができました。また、さらに彼らの専門知識を深めることで、自ら講義ができるスキルの高い取得者を育成することができました。このようにCISSP認定資格の導入により、社内の人的リソースを使って、技術者のスキルを向上させ

られることを日立グループ全体にアピールし、もともと充実していた社内教育プログラムに、CISSPのインハウスセミナーおよび (ISC)²公式CISSP10ドメインレビューセミナーを加えてもらうことを計画しています。現在当社には150名のセキュリティ技術者が在席していますが、内19名のCISSP認定保持者を将来的には50名ほどに増やそうと思っています。

CISSP認定資格で得た幅広い知識を活かし、セキュリティハイパーレスキューチームを結成

私たちがインハウスセミナーを開催してまで、CISSP認定資格を普及させたいのは、CISSP認定資格取得の過程で情報セキュリティの共通言語を習得できると考えたからです。日本のセキュリティ・システム技術者の多くが、アプリケーションやネットワークから入っており、技術的な知識に片寄っています。一方、最近SOX法などが施行され、コンサルタント業務が増えています。その際、法令や規制、基準に精通していない、あるいは専門外のファイアウォールや暗号などのテクノロジーを理解していない技術者が増えています。その点、CISSP認定保持者は、情報セキュリティ・プロフェッショナルに求められるグローバルレベルの共通知識(CBK)を整理したCISSP10ドメインを学習しており、セキュリティ全体を万遍なく体系的に理解しています。CISSP同士

であれば、このCBKを共通言語にして、世界中の製品ベンダーや外部コンサルタントと会話でき、そのことで信頼度の向上にも繋がります。私たちはこのような幅広い専門知識を身につけたCISSPの中から、セキュリティ事故の緊急対応を3回以上経験した10名を選抜し、セキュリティハイパーレスキューチーム「SHIELD110番」を結成しました。機密情報の漏えいやスパムメールなどのセキュリティ事故などに対応し、企業から緊急対応の要請があった際、顧客先に出向いて状況を調査。対応策を迅速に提示することで事態を早期に沈静化させます。チーム結成のきっかけは、地震などの災害時に機動力を発揮する、特別な技術と能力を持ったハイパーレスキュー隊にインスピレーションを受けたことです。

2010年までの中期目標を達成するために今後もCISSPを活用し続けます

当社の2010年までの中期目標のひとつに、セキュリティ分野を飛躍的に伸ばすという計画があります。そのための施策としてCISSP認定資格取得サポートを行い、具体策として先ほど述べた「SHIELD 110番」を設置しました。このような成長が期待できる、時代を先取りした情報セキュリティサービ

スを提供できるのもCISSP認定資格を導入し、セキュリティ技術者のスキルを底上げできた結果だと思えます。今後は、社会全体の危機管理意識の向上を背景に、情報セキュリティのプロフェッショナルに対するニーズの高まりに応えるために、CISSP認定資格の取得率を上げていこうと考えています。