

グローバルビジネス環境において「総合リスクマネジメントソリューション」を提供するトッププレイヤーを目指す

NTTコミュニケーションズ株式会社 / NTTコムセキュリティ株式会社

NTTコミュニケーションズ株式会社は、国内で最多数のCISSP取得者を擁する企業です。前回（2007年11月）、インタビューを実施した際には2010年に向けた事業ビジョンを実現するためにはセキュリティ分野のエキスパートの育成が不可欠であり、その原動力としてCISSPが大いに役立っていると評価されました。

今回はあらためて、同社の経営企画部・マネージドセキュリティサービス推進室担当部長であり、NTTコムセキュリティ株式会社の代表取締役社長も務める、竹内文孝氏に取材しました。「ビジョン2015」の実現に向け、グローバルビジネス環境において「総合リスクマネジメントソリューション」を提供するトッププレイヤーを目指す同社の営みと、かかる取り組みにおけるCISSPの役割について語っていただきました。

Q 貴社のビジネス背景についてお聞かせください。

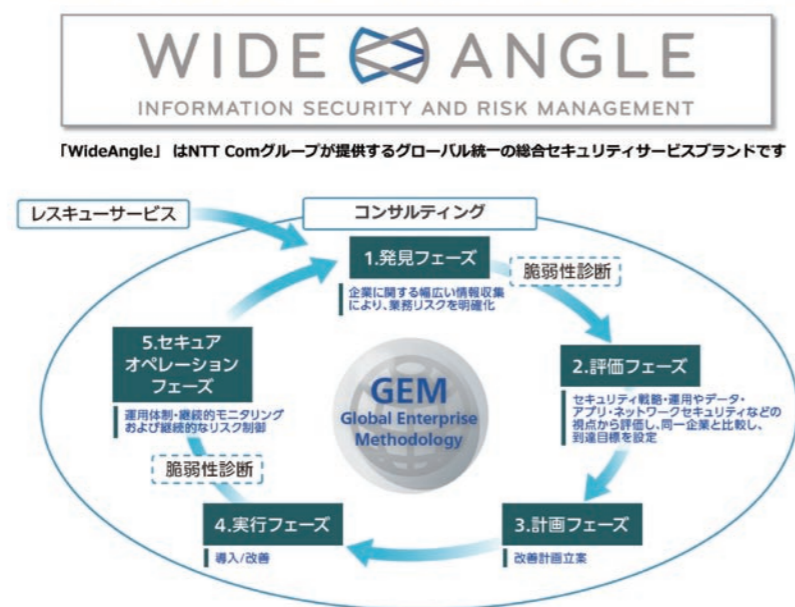
NTTコミュニケーションズ（以下NTTコム）は、2003年に東京SOC（セキュリティ・オペレーション・センター）を立ち上げ、セキュリティサービスを展開してきました。2009年までは日本、アジアの日系の顧客企業を対象にセキュリティ・オペレーション業務のアウトソーシングサービスを提供してきました。私自身、東京SOCの立ち上げに携わってきました。

2009年にドイツのIntegralis社を、2010年にはスウェーデンに本社のあるSecode社を相次ぎ買収しました。2012年に、東京SOCとIntegralis社、Secode社の三者のサービス統合を行い、翌2013年には事業体も統合し、設立されたのがNTT Com Security（NTTコムセキュリティ）です。NTTコムセキュリティの持株本社はドイツにあり、15カ国に事業会社、地域会社を持っています。NTTコムセキュリティ株式会社はその事業会社の一つです。

2013年のNTTコムセキュリティの設立とともに、NTTコムグループのグローバル統一の総合セキュリティサービスブランドとして「WideAngle」を立ち上げました。

「WideAngle」は顧客企業のICT環境のセキュリティレベルを把握し改善する「プロフェッショナルサービス」「セキュリティ対策の提供サービス」「SIEM（Security Incident and Event Management / セキュリティ関連の各種情報の管理、相関分析）エンジンを活用した「マネージドセキュリティサービス（MSS）」を「総合リスクマネジメントサービス」として提供します。海外で25年にわたり8,000件以上の実績を誇る「コンサルティング」をはじめ、セキュリティインシデント時の復旧作業を支援する「レスキューサービス」、ICT環

NTTコムの総合リスクマネジメントソリューション

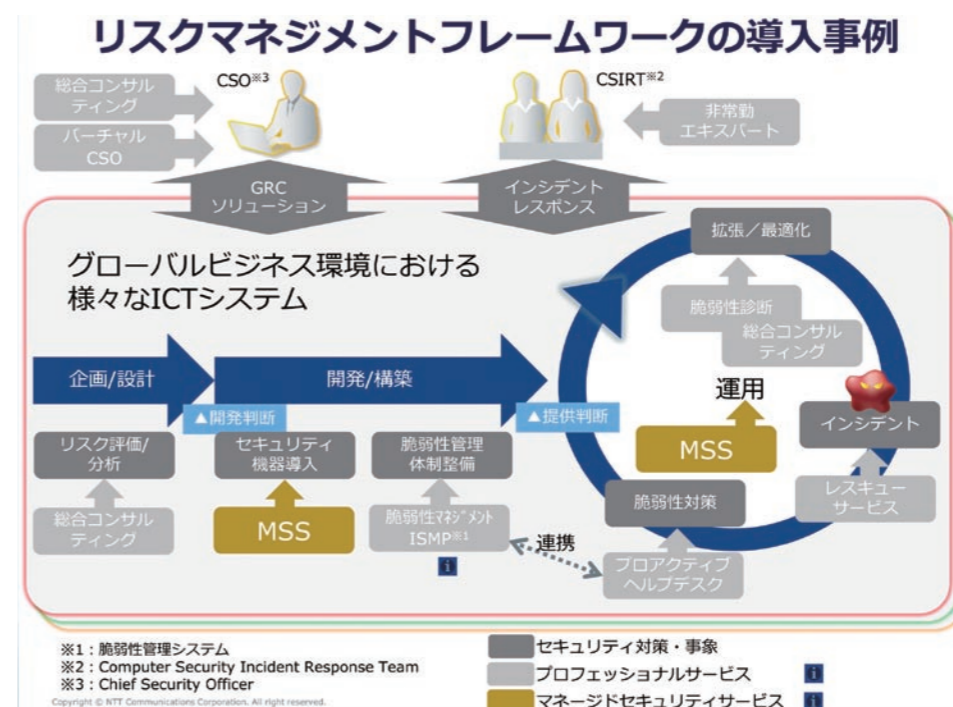


NTTコミュニケーションズ株式会社
経営企画部
マネージドセキュリティサービス推進室
担当部長

NTTコムセキュリティ株式会社
代表取締役社長
CISSP
竹内 文孝氏

境の弱点を可視化する「脆弱性診断」からなる、世界15か国800名の経験豊富なセキュリティコンサルタント・エンジニアによる専門性の高いセキュリティサービスです。経営層はグローバルビジネス環境において、常に事故が発生することを前提にセキュリティリスクを最小化できるフ

レームワークを考え、常にリーダーシップを発揮しなければなりません。企業は、何十何百というICTシステムを内包し運用しています。いわゆるシステム開発ライフサイクルがあり、一つひとつのシステムを一元的に管理するCSO体制、問題発生時の



CSIRT体制は当然あるのですが、これらの体制に応じたセキュリティライフサイクルも必要だということです。どのような企業でも、システムを企画・設計し開発していくうえでの経営判断があり、経営判断するにも「この設計でセキュリティ面は大丈夫なのか」といった、リスク評価、分析を必ず実施しなければなりません。情報セキュリティとリスクマネジメント活動をシステム開発ライフサイクルに組み込むため、統制のとれた構造化されたプロセスを提供できるリスクマネジメント・フレームワークの確立が必要なのです。かかるフレームワーク全てに提供できるメニューを備えているのが「WideAngle」なのです。

事業ビジョン実現のために CISSPホルダーの増員は喫緊の課題 人材育成の推奨プログラムの中に CISSPを組み込む

Q 貴社のCISSP資格を推奨する目的と、その意義付けについてお聞かせください。

グローバルで一定レベルのサービスを顧客企業にシームレスに提供する際に、CISSPは必要不可欠なものと考えています。採用、配属する場合などCISSP取得者であるか否かが一つの大きなポイントになります。日頃のメーカー、SIベンダーとの取引においても名刺にCISSPと記載されているだけで、「言葉が通じる」、「技術レベルが同等だ」という共通認識を持つことができます。特に欧米のビジネスパーソンとの間では、「固く握手ができる」という雰囲気を感じることが多々あります。

NTTコムセキュリティは、コンサルタント200人中20人ほどがCISSPを取得しています。担当する業務はさまざまですが、コンサルタント、準コンサルタントの位置付けで海外でも使用している厚手のプレミアム感のある名刺を持たせています。CISSPホルダーとしての誇りと責任を持ってもらうための一つの工夫です。



Q 人材育成に対するお考えと、人材育成のプロセスにおけるCISSP取得効果についてお聞かせください。

セキュリティ分野においても人が重要です。いかに人材を育成していくかが、私たちの最重要課題です。目指す人間像は、グローバルで通用する「アナリスト型セキュリティ人材」と「組織マネジメント型セキュリティ人材」です。

人材育成の取り組みは、採用の時から始まります。採用時にセキュリティに興味を持っている人間であるかどうかを

まず確認します。「セキュリティに興味を持っている」とは、例えば、「現在のあなたの家庭のパソコン環境、ICT環境はどういうものですか?」といった、実際にセキュリティについてどの程度興味をもって生活しているのか、取り組んでいるのかを掘り下げて聞くようにしています。

採用後には研修を行います。NTTコムは、独自に調査研究を中心に行う部隊、先端IPアーキテクチャセンター (IAC) という部門を持っています。ここでセキュリティエンジニアリングの基礎力習得に向け、基礎的な技術から始まり3カ月程度のブートキャンプのプログラムを実施したうえで、配属となります。もちろん、配属後もOJTなどでノウハウを習得しつつ、デフコン (DefCon) やさまざまなセキュリティ関連研修に参加させて資格を取得させるようにしています。

NTTコムでは、2007年度よりプロフェッショナル人材育成プログラムを立ち上げ、社員の育成を行っています。2012年度からは専門分野を細分化し、社員個々が目指す専門分野と人材像をより詳細に設定しました。その中にはセキュリティエンジニアという専門分野もあります。

このプログラムの中では、社員のスキルを判定するためのスキル診断も行っており、診断結果に基づいて社員は0から3までの「マイルストーン」の認定を受けます。ちなみに、1以上のマイルストーンに認定されれば、認定一時金が支払われます。このように目指すべき人材像や基準を定義することで、社員にはプロフェッショナルを目指させます。これは正にCISSPで重視されている内容と重なります。

また、スキル診断は社員それぞれの専門分野に基づいて社内と社外の基準での診断があるのですが、社外基準では資格による認定を設けています。CISSPも対象資格として採用されており、前述したセキュリティエンジニアの専門分野では社外基準のマイルストーン1相当として設定しています。つまりセキュリティエンジニアでマイルストーンを獲得したければ、「CISSPをまず取得しなさい」と勧めているのと同じです。

Q 今後、CISSP認定保持者をどのように増やしていこうとお考えですか?

2010年以降、人材育成のプログラムの中にCISSPが組み込まれ、推奨プログラムになっています。CISSPは高度な資格ですし、研修も受けなければなりません。資格を維持するのも容易ではありませんので、かかる取り組みにおける費用は基本的には会社が全て負担することとしています。もちろん、無条件ではなく、キャリアプランを作り、選抜されたメン

バーを対象とします。その選抜に至るまでの段階でも、全社的なプログラムとしてモチベーションを持たせる仕組みを構築しています。簡単に取れる資格ではありませんので、計画的に取り組みつつCISSPホルダーを大幅に増やしていきたいと考えています。

Q 最後に、今後の展望を、CISSPとの関連でお聞かせください。

近年、企業における情報セキュリティリスクマネジメントは経営課題であり、GRC(ガバナンス、リスク管理、コンプライアンス)ソリューションへの期待は高まる傾向にあります。いくつかの企業顧客の事例をみても、現行システムの脆弱性が突発的に発見され、その対応に苦慮、苦戦する事態に遭遇することが頻繁に起きていると言えます。このような環境下では、リスクの定量的な評価や対策立案の体制が必要であり、問題発生時には迅速・的確に、かつ組織的に行動できる準備が欠かせません。

つまり、情報セキュリティやリスクマネジメントに関する幅広い知識を持ち、網羅的に課題に取り組める人材が求められており、今後ますますCISSPが非常に大きな力を発揮するのではないかと期待しています。

前述の「WideAngle」は、コンサルティング、GRCソリューションとMSSが一体となった他に例のないサービスです。この特異性を活かし、事業の成長を図るためには、顧客の上層部と経営に関する会話ができ、かつセキュリティに対して網羅的に精通するレベルが求められ、ゆえにCISSPホルダーの増員は必須だと認識しています。

また、一般の企業においても、消防や安全衛生の管理者が必ず配置されているように、情報セキュリティの責任者の設置も当然の時代も近いと感じており、CISSPへの需要は高まるばかりであると考えております。

セキュリティ人材育成モデル

- ▶グローバル人材に加え、セキュリティ人材¹⁾の採用による有望層拡大 (NTT Com Securityも活用)
- ▶研修等を通じたグローバル・セキュリティ両能力を兼ね備える人材の育成を図る
- ▶複数業務のOJTによる総合的なセキュリティ力の修得を推進
- ▶リーダ業務の実践を通じて、マネジメント力も兼ね備えた人材へと昇華を図る

