第６回目　サイバーセキュリティー研究会
実施日：２０１８年１２月１２日（水）
発表者：横浜 信一氏　NTT CISO (Chief Information Security Officer)
発表テーマ：「産業界におけるセキュリティ人材育成策」
会場：機械振興会館 5 階　5S－2 会議室

本研究会メンバーの一員である横浜氏よりサイバーセキュリティ人材について下記の項目・内容でご発表いただいた。その後参加者からの質疑応答及び様々な意見交換がなされた。

1.発表報告

<サイバーセキュリティー人材の用語定義と求められる人材像>
サイバーセキュリティ人材育成策はビジネスや経営管理などのコンテキストから幅広く捉えることで用語に対する解釈や共通認識を浸透させる必要がある。具体的には、サイバーセキュリティはアーキテクチャーやテクノロジーなど物作りにおける技術設計上の課題ではなく、デジタル社会において日本のビジネス環境に立ちはだかる課題である。したがって、人材育成はコンピューターやネットワーク実装・設計など技術的専門家に偏るのではなく、会社や組織経営に携わる取締役・重役、従業員、さらに取引顧客などの社外関係者やステークスホルダー全てを含んだ包括的なものであることが望ましい。

まず肝心となるのが、会社経営の舵取りを担う取締役、理事・役員、経営執行レベルにおける意識的改革である。日本は欧米に比べて役員クラスにおけるセキュリティについてのミーティングが乏しく、２周回分遅れている。サイバーセキュリティをビジネス・社会的リスクとして全面的に取り入れ、そのための適切なガバナンス、組織編成、意思決定、社内外におけるアクションやアカウンタビリティは欠かせない。社内取り締まり役であれば、執行陣に対して問題を問いかけ、適切なアクションを取らせることが要求される。株主や会計監査役、法務アドバイザーのように外部から経営に関わる場合は、適任した取り締まり役の選任や、内部におけるリスクモニタリングや不正や異常稼働に対する取り締まり役への追求がそうである。

経営執行層であれば、サイバーセキュリティを組織全体の専門業務として統括するために CISO を置き、それを元にサポートやスタッフチームを形成できるようにするが重要である。その際、他の経営執行者に対してサイバーセキュリティに対する正しい理解や業務執行に伴うサポートを得られる様に密接なコミュニケーション（氏曰く、精神的にハードルが高く非常に難しいとされているが）が大切となる。同時に外部委託か社内持参の意思決

定、アウトソースの際に必要となる情報や物品など全体的に把握していなければならない。

その下に位置するセキュリティ専門チーム(CIST)には、テクノロジーにおけるエキスパートの他に、NIST の定型的５ステップ（守るものの優先順位化、防衛プラン立案、モニタリング、復旧に向けた早急対応、行動のルール化）や社内外、他組織からの連絡口として役割が重要になる。その際セキュリティ至上主義にならないように、企業文化に密着させたパートナーシップを築き上げることが大切である。

次のサプライチェーンだが、従来までは取引先の顧客もしくは部外者と見られてきていたものである。ここ十数年のビジネスの大きな変化により、現在では企業活動の一部となっている。部品やファシリティ管理、システムインテグレーターなど製造・管理・運営など業務上のあらゆるところで密接に関わっている。そのため、企業元の調達部門はサプライチェーンを部外者ではなく、企業利益共有者の一員としてプロテクトする必要が出てくる。

最後に一番下の全ての従業員が人材として重要な役割を担っていることは言うまでもない。一般的には従業員はメール添付の開封や IT 部門から指定されたソフト以外のプログラムインストールやアップデートなど何気ない所で日常的にセキュリティ脆弱性リスクに直面している。セキュリティ認知と理解を深めるための社内における適切な対応法や訓練、アカウンタビリティ設置など定期的に行うことが大切である。

<産業界における現在の人材育成の取組み>

２０１６年より産業横断型の人材育成検討会を発足。重要インフラ企業を中心に電気・通信事業・OA 機器・プリンタ・自動車・保険・金融・消費サービスなど系４８の大手企業が加盟。産業横断型で、日本のビジネス慣習に合わせた必要な人材の定義やガイドラインなどについて協議を行っている。２０１６年に第一次報告書が発行され、全タスクや役割の洗い出し、セキュリティ統括室設置の必要性などを提言した。その他には、日本 CSIRT 協議会主催による短期型（２泊３日）セミナー（組織運営・技術・法律などのモジュール別研修）や情報セキュリティ大学院大学による社会人向けの修士や短期集中型コースの提供、ISAC（業界ごと）、ネットワークセキュリティ協会、IPA、一橋大 MBA、gacco(MOOC：Massive Open Online Course）などを通じて人材育成の場を提供している。

<NTT における取組み>

NTT では持ち株会社とグループのシステムを生かした独自のセキュリティ体制を構成している。NTT グループの各企業に CISO が置かれており、グループ全体には CISO コミッティーが存在する。NTT のセキュリティ体制は、社内を守るためのセキュリティと顧客へのサービス提供を目指したセキュリティといういわゆる二重のミッションである。サービス開発・運用部門にセキュリティ全般を請け負うスペシャルチームを設置し、顧客の場合は営業・顧客サービス部門への対応（地域・業界別）、社内の場合はコーポレート部門下の CISO との連携により育成や社内トレーニング、緊急対応などを通常業務として行っている。

社内の人材トレーニングは独自に体系化したものを取り込んでいる。人材タイプを３つのカテゴリー（セキュリティマネージメント・コンサルティング、社内運用、開発研究の）に分け、それぞれで３レベル（初級・中級・上級）に分けている。共通のロゴとレベル別に色分けした認定証を発行することで、グループ全社員におけるセキュリティ人材の質的な底上げとプログラムの改善に努めている。ちなみに NTT 全体における日本人の人材の質は、初級レベル４万人、中級レベル３０００人、上級３０人という分布である。初級レベルはオンライン学習の受講とチェックテスト、中級レベルはセキュリティ業務に関連したもので業務上の法律と技術面における内容把握・知識習得が中心となる。上級レベルは、ホワイトハッカーチームのように研究所に籍を置き、マルウェア解析、ソフトウェア分析高官、海外ハッキングコンテストへの参加、社内セキュリティ担当への冊子マニュアル作成、セキュリティコンサルティングなど技術的に高度な実務に携わるなど少数精鋭のスペシャリストである。

＜人材流出について＞

- 日本の多くの会社と同様に、NTT でも人材流出は起きているが、日本を守りたいという強い正義感やグローバル企業にて同じミッションを持った人との出会う機会などから残る社員もおり、キャリアパスに対する捉え方はまちまちである。
- NTT を出て行く人はセキュリティ重視による研究への圧迫感や業務ネットワークプラットフォームの環境の取り扱いに対する是非、社内の官僚・役人的プロセスへの不満などが挙がっている。

2.質疑応答、参加者からのコメント

- 人材流出に対する組織的なアクションは何か行なっているか？

  研究所の IT 環境に問題があり自由な研究の妨げになっているので、その見直しを提案したいと考えている。研究所は Linux で社内 WindowOS で環境整備を行うのに極めて労力がかかっている。人材育成の評価については人事制度にまだ完全に適用されていないので今後考えていきたい。

- 後継者の育成についてはどうしているのか？

  人によって任せている。１０年から１５年でどうなるということは一概は言えないが、３年のスパンでトレーニングを行っており層は厚くなっている。

- スペシャリストの全てにおいて代替わりが必要というわけではない。中には憧れてその道を追い求めてきた結果今ここにいるという人たちもいるので、今後必要とされている人材領域における次のエキスパートが育っていけばそれで十分だと思う。１０年後に上級レベルに上がって来るという仕組みが出来上がれば理にかなう。

  現在では具体的どこに何人必要で予算をどの程度見積るというレベルの青写真はまだ出来上がっていない。

- セキュリティリソースに対する将来的な予測や見積もりは短期間で行えるものなのか？

  正直いうと自分でもわからない。ただ CISO となるとなんらかの形で持っていないと始まらないというのが率直な感想である。

- 特殊領域に精通した人材を引きとどめるための手は何かあるか？

  一案として Red Team の形成を検討している。これは会社の中で登り詰めるのではなく、特定分野で一流を目指すという人向けにしたアイデアである。会社での任務と同時に個人でやりたい研究を好きにやらせるという自由度をもたせすることでリテンションにつながるのではないかと考えている。そうすることでサイバー攻撃に対する訓練や防衛力向上にもつながり会社全体にとっても大きなプラスとなる。だた問題はシミュレーションとして寸止め対応で社内全体で実行できるものなのかどうかだが。

- セキュリティ制度として何か保証を社内で設けているか？

  上級の上をランクとしてを設けた。現在 5 人ほど。

- NTT で研究者の中からマネージメントに上がって来る人はいるのか？

  NTT ではそういう道をたどる人は珍しくない。私のチームは人事異動の中で入って来ているが、スペシャリストの人たちはそれぞれの領域の中で社員として機能している。NTT の場合は業務上の性質から尖った人材とジェネラルリストの両方が必要だが、普通の会社では前者はいらないので、サラリーマンとしてどうセキュリティに精通させるかというレベルであれば、産業育成検討会のような事例を追求した方がいい。

- NTT ではどの専門分野が強いのか？

  ネットワークやソフトウェアに強いが、ファームウェアや IC チップの内部構造などについては余りに強くはないと思う。ソフトウェアエンジニアリングや情報工学を主なベースとしてスペシャリストを発掘している。

- スペシャリスト待遇について会社側に横浜氏の後任者についての将来的な考えはあるか？

おそらく会社はそこまで考えていないと思う。仮に私が辞めたとなると後任には技術戦略副社長が兼任として来るというようなことが出て来ると思う。私が在籍間に組織全体として周りの仕組みを作っておく必要があるかもしれない。

- NTT でトップエンジニアとして数えられている人たちはあくまでも CC-CERT のフォロワーであって CC-CERT ではない。だから上に誰がつこうが、彼らの業務・研究に影響を及ぼさない限り（経営・管理層に対して）怒ることはない。上の後任についての話となると CC-CERT の内部と CISO との関係の話になるので、全くとは言わないが組織編成上の問題に巻き込まれることはないと思う。

- 今回の話は尖った人材が中心だが、技術とマネジメント両方においてセキュリティ分野の仕事ができる人材が育成できるかということも重要な点として取り上げたい。過去に業務上の依頼で NTT セキュアからサービスマン 2 人に出向してもらった時に、手際の良い対応をしてくれた経験がある。尖った人たちではないが、技術・マネジメント双方において二人とも大変優秀という印象を持った。個人的にはこういった現場でのサービス対応などでより多くの人材が育ってきて欲しい。バランスのとれた人をどう育てるかについて興味があり、非常に重要な課題といえる。

- NTT を卒業して CISO になった人はいるか？

  NTT データを辞めて CIO を経由し CISO になったケースが一つある。うちからは現在 LINE でセキュリティヘッドについている者がいるが、CISO ではない。
- 日本では CISO という名前が出てまだ１０年程度しか経っていないので、現在そんなに必要かどうかというような印象はまだ持たない。
- NTT と同じようにパブリックアドボカシーなど積極的に外に発信するような企業やチームはあるか？

  私の知る限りでは東京電力の CISO。今後のセキュリティ活動について対外コミュニケーションを行なっている。チームとしては DeNA のセキュリティ執行者で、会社のセキュリティ対策についての本まで出版している。

＜サイバーセキュリティに対するメディアの取り扱いについて＞

- NTT に尋ねて来る人はいるか？

  なぜ大きく取り扱われないのか、勉強したいので教えて欲しいとうちに尋ねて来た人は数人いる。
- メディアの取り扱いに関する情報専門誌はあるのか？

  欧米には専門誌が数多く出ている。オンラインでも入手可能。日本だと日経コミュニケーションとかでたまに出て来る程度だと思う。
- サイバーセキュリティについて一般人に説明するのが難しいという声をよく聞く。

重大インシデントの際に持ち株会社全体として、技術だけではなく総務、経理、法務など全てにおいてセキュリティチームを置き、守るべき情報・資産などについて意識や考え方の擦り合わせを定期的に行なっている。