第５回目　サイバーセキュリティー研究会
実施日：２０１８年１１月１４日（水）
発表者：衛藤　将史氏　NICT(国立研究開発法人情報通信研究機構)
ナショナルサイバートレーニングセンターサイバートレーニング研究室室長

総務省近藤氏の紹介で特別参加。衛藤氏はネットワークを中心とした先端技術研究を専門とし、ネットワーク、ルーティング、Web セキュリティの標準化などを中心に携わってきた。国家行政主体で行っている持続的セキュリティ人材の供給についてご発表いただいた。NICT 行政法の改定後、２０１６年より人材育成・教育事業を立ち上げる。２０１７年より若手に向けた人材育成の仕掛け作り（セキュリティキャンプ、SECCON, SecCap, CYDER など）を開始。後半に NICT における人材育成の取組みについてお話しいただいた。

＜国内におけるサイバーセキュリティ人材教育・育成トレーニングとその現状＞
日本における人材育成プログラムは、勉強会、研究会、協議会レベルのコンテスト（国内で１３箇所、国内最大レベルは SecCap）などがある。その多くは有志レベルで行われている。勉強会やイベントでは以下３点をアピールしている。
- 人脈・ネットワーク

セキュリティ情報の外部発信することに対する意識改革の重要性
人脈ネットワーク作りはセキュリティ業界において必要不可欠
SecCap 学生をオフラインで集めて招集。SecCap におけるリピート参加
- 共通のデータセットの提供

NWS では共通データセットを入手し、学生に配布。
- セキュリティコンテストの実施

1. サイバーセキュリティ人材をめぐる現状分析
民間レベルで行っている人材育成と重なっていないか？排出側（育成部門側）と民間・ユーザー企業側のニーズは合致しているかどうかを中心に調査した。国内６つの人材育成プロジェクトについて人材のマッチングについて分析・ヒアリングが行った結果、以下のようなことが判明した。
- SECCON における高度技術(Forensics やバイナリ解析）による実績があっても、ユーザー企業では求められていないことが非常に多く、受け入れてもらえない。仮に受け入れられてもさせてもらえないため、長く続かずに辞めてしまう。
- SecCap 発足当時は質的に少数精鋭でスタートしたことからレベルが高かった。参加大学の数をいたずらに増やすと相対的に学生の動機付けが下がり、質的維持が難しくなる。

- CYDER のような実践的演習は人を増やそうとするとコスト負担が大きくなる。有料にすると受講を拒否する生徒が出てくる。

＜育成側と企業側における人材ニーズの違い＞
人材育成側、企業側の双方とも現場寄りという意識は共通しているものの、需要と供給におけるくい違いが存在している。人材育成側はジェネラリストニーズはあるものの、企業側のように第一優先ではない。専門分野における研究の追求を求める学生と企業とでは領域的に思惑が異なっているのが現状である。

人材育成側：現場寄り、ニーズは幅広い
ユーザー企業側：現場寄り。ジェネラリスト

＜技術領域におけるニーズ＞
人材育成側：ユーザー企業ほど、ストラテジー・ガバナンスのニーズは少ない
ユーザー企業側：ストラテジー・ガバナンスの知識を持っている学生を要望

高：ネットワークセキュリティ、ストラテジー・ガバナンス
低：フォレンジックス・バイナリ解析

2. NICT における人材育成の取り組み
- ２０１７年４月発足
- セキュリティーオペレーターとイノベーター双方の育成

A.CYDER
＜対象＞国家及び地方公共団体 C-SIRT 担当者・従事者
２０１６年より NICT 主催。年間１００回、全国４７県、３０００名（一回３０名）2013年よりパイロットプログラムとして開始。

CYDER トレーニング：オンライン講習（約 1 時間）と演習舞台の設定
昨年の例としては STARBED を駆使し、Juki-Net を想定した Apach 2 脆弱性対応について演習を行なった。そのほか Sky-C 脆弱性、持ち込み PC などによるシナリオも用意。

B. Cyber Colosseo
＜対象＞Olympic Games in Tokyo 2020 運営組織委員会
サイバー攻撃の増大が予想される。データ解析やバイナリなど高度レベルの技術も用意し、

攻撃に対する防御法や組織委員会のネットワーク環境の保護など幅広く実施。

C. SecHack365
＜対象＞２５歳以下の若手を対象とした継続的ハッカソン（創造的人材の育成）
５０名を国指定として選抜　４月～６月にかけて全国に公募。２ヶ月に１度集まる。
メインはオンライン環境における演習・教育（マルウェア解析など)。

CYDER を通した人材育成：年間３０００名
（２０２０年までに必要とされるセキュリティ人材２０万人）
- 民間企業者は有償を条件に参加
- 開発者育成を狙いとした若手強化

日本国内におけるセキュリティ産業は海外からの製品が圧倒的に多く、将来的には国内で生み出せるものを作り出していく必要がある。

質問・意見・コメント
＜人材育成領域・研修トレーニングについて＞
- ユーザー企業側にとっては技術専門やスペシャリストは抱えたいのではなく、いざ困った時にいてほしいというのが率直な印象ではないか。政策上育成の大きな対象になるのは文系出身者なのだから、経営者側に対してコンピューターリタラシーや事故対応方法などを提供する仕組みが必要だと思う。
- NICT は高い技術領域による研究開発や教育を提供しているが、これを会社経営などオペレーション上の観点から光を当てるということはできないのか？
- セキュリティ事業における職種やスキルアップはどのようにして行われているか？
- 入社研修時点でガバナンスやストラテジー向けに研修するといったことは行っているのか？
- 企業へのサイバー攻撃と想定した演習をモデル化して売り込むことはできないか？（座学で終わらせるのではなく、事故が起こり、プレス報道され、企業利益の影響、社長による謝罪までを設定したシナリオまでを導入するなど）
- 経営学部向けのケーススタディを提供してみたらどうか？
- Public Relation 向けに提供するなどカスタマイズできるものがあるのもいい（例えば事故が起きた際のメディアに対する事業管理者の対応法など)。会社による事情（雇える・雇えない）もあるが管理職研修で対応することは不可能ではない。

＜セキュリティー人材２０万人に対する意見＞

- ２０万人も必要というメッセージには根本的に疑問がある。セキュリティエンジニアはそんなにいるものなのか？
- ユーザー企業側、ベンダー側、中間管理層側などによって人材に対する解釈はまばらである。頭数が先走っている感があり、根底にコンペテンシーに対する意識的問題があるような気がする。
- これは NICT 事業の最大の課題であるが、年間の母数が不明で３０００人トレーニングすることの必要性と意義が見い出せていないのが現状である。
- NISC による数字はアメリカにおけるセキュリティ求人の数を参考にしてもらった経緯があり、日本におけるセキュリティ環境から汲み取ったものではないことがわかる。
- C-SIRT 初級・中級者に対象人数を限定して出した方が効果的だと思う。

＜カリキュラム作成・シナリオ設定について＞

- 日本国内において英語でレクチャーやトレーニングの提供をできるところは民間や SepCon などの一部のイベントを除くと殆どない。NICT でも行っていない。
- 演習シナリオは攻撃に関する事例はよく出ているが、事後対応などはついては受講者への教育上、個人情報への懸念もあり、実名で出すのは難しい。
- 実存する詐欺 Web サイトなど実情報を事例やシナリオ設定に取り込むといい。
- NICT でなければ実現できないものを洗い出して、外部に売り出すのも良いのでは？