ASIS インターナショナル日本支部
広報担当理事　長瀬　泰郎

# ASIS インターナショナル日本支部便り

## 月次セミナー　１月度 「情報セキュリティと物的セキュリティ」

一般に物的セキュリティと情報セキュリティは、全く異質のものと考えられることが多いのではないでしょうか。しかも、インターネットで検索すると圧倒的に情報系のものが沢山出てきます。物的セキュリティの占める割合はわずかです。しかし、実際には考え方の根底は同じなのです。

１月の月次セキュリティミーティング講師はコロムビア　ミュージック　エンタテインメントの情報セキュリティコンサルタント、ニール・ボトナク氏です。氏は物的セキュリティ分野にも豊富な経験と深い造詣を持っており、２つの分野の類似性と相違について大いに語ってくれました。「CTO in the box」（びっくり箱から飛び出す情報セキュリティ幹部）の異名をもつボトナク氏の奥深いセキュリティ論とコンピューター、ネットワーク、ファイアウォールの基本についての話です。

講演するニール・ボトナク氏

### ■似ている点

- ファイアウォール＝インターロック
- ウィルスチェッカー＝監査と爆弾処理班
- 侵入検知システム＝監視カメラとセンサー
- ネットワークスキャナー＝巡回
- 暗号化＝金庫と鎧
- エクスプロイト＝武器
- アクセス制御＝出入管理
- トロイの木馬＝爆発物

### ■共通に使われる用語

- 照合（Identification）
- 認証（Authentication/Authorization）
- アクセス管理（Access Control）
- 証跡（Forensics）
- 脅威（Threats）
- 脆弱性（Vulnerabilities）
- リスク分析（Risk Assessment）

### ■情報系に特別のもの

- **6 分間ルール（6 minutes rule）**
  ハニーネットプロジェクトで明らかにされたことですが、パッチなし Windows システムをインターネットに放り込むと平均わずか 6 分で乗っ取られてしまいます。インターネットの世界がいかに敵意に満ち溢れているかを示す実験です。
- **自律エージェント（Autonomous Agents）**
  製作者の意思とは別に独立して動くプログラムです。一部はウィルスとして準受動的に、もう

ひとつはワームとして能動的に活動します。ウィルスは生体ウィルスに似ています。Word 文書などのプログラムに乗り、E メールなどで広がり、形を変えて防御メカニズムを攻撃します。一方、ワームは、メールなどには付かず、直接ネットワークから攻撃をします。最近は極めて巧妙化しており、複数ルートで運ばれたり、同時攻撃を行います。

熱心に聴く参加者

- **無差別（Indiscriminate）**
  犯罪の世界では、狙うターゲットに一定の条件があります。お金持ちだとか、守りが弱いといったことです。しかし、インターネットの世界では、攻撃対象は誰でもよく、しかも自動的に攻撃を行います。ハッカーはストレージ、情報、お金、そしてゾンビを欲しがります。ゾンビとはハッカーが操るPCのことです。ゾンビの軍団のことは BOTNET と呼ばれます。
  どんな PC でもどこかに脆弱なソフトウェアを持っていますから、自動攻撃機能によってハッカーが寝ていても攻撃を続けられるのです。攻撃は無差別に行われます。インターネットの世界ではみんながお金持ちで守りが弱いので、攻撃する PC は 1 台でも百万台でも、手間は同じです。
- **事案対応（Incident Response）**
  ハッカーは自分の身を隠して間接的に攻撃するため、被害者の PC を攻撃者として仕立て上げるのです。このため、犯人に対して反撃しても、結局無実の人を傷つけるだけに終わってしまいます。警察にはこれまでにない技術力の強化が求められます。サーバー押収する程度のことでは追いつかないのです。
- **求められる非硬質な環境とツール（Non-Hardened Environments/Tools）**
  インターネットは極めて敵意を持った環境なので、ほとんどのソフトウェアはそこからの攻撃に対する脆弱性を持っているので、徒手空拳でこの世界に入るのは乗用車に乗って戦場に行くようなものです。

## ■情報セキュリティ文化（Infosec Culture）

- **現状**
  まだ若い産業なので、共通用語もまだ確立していません。また、時代の流れが速く、よい概念もすぐに色褪せてしまいます。そして情報セキュリティ世界は砂上の楼閣のようなものです。
- **三種類の人（White, Black and Grey Hats）**
  善人（White）は法を守り、防御に努めます。悪人（Black）は法を破り攻撃者となります。そして、その中間の人（Grey Hats）がいます。
  それぞれのグループに属する優れた人材は、お互いをよく知り、連絡を取り合ったり、会議やコンファレンスで接触することもあるのです。また、一人で二役、三役を務める人もいます。

会場の様子

- **全面開示（Full Disclosure）**
  これからのセキュリティ研究者は、脆弱性情報を詳細にわたって公開するようになります。研究者の間では、公開しない限りバグを潰すことができないことが経験的に知られており、「責任公開」を行うようになりました。責任公開とは、問題をベンダーに直接通知し、パッチが開発されたら問題の詳細を公開することです。
- **ピアレビュー（Peer Review）**
  しっかりセキュリティ対策されているソフトウェアは世界中の研究者によってレビューされています。ピアレビューされていない暗号アルゴリズムは無価値だし、監査ができないプログラムは信頼できないのです。
- **情報セキュリティにおける基本原則（CIA）**
  秘匿性（Confidentiality）、完全性（Integrity）、可用性（Availability）の三つは、情報セキュリティの攻撃側と防御側の両方に当てはまる原則です。

## ■ 情報セキュリティと物的セキュリティの比較まとめ

- 両者は基本的に同じもの
- 対策のとり方と用いるツールは異なる
- インターネットは極めて危険な環境
- 最近の PC は攻撃に脆い
- 情報セキュリティの世界は常に変化しており、ますます対策が難しくなっている。
- しかし、物的セキュリティに比べ、情報セキュリティの世界の方がずっとオープンである。
- 結論的に言うと「セキュリティは幻想だ（Security is an Illusion.）」

ボトナク氏の通訳をする筆者と菅谷さゆりさん

今月のセミナーは、インターネット環境と情報セキュリティについて、悲観的な話題が多かったようです。2 月のセミナーは、具体的に私たちが自分と会社のコンピューターを守るためにできることを前向きに取り上げます。どうぞお楽しみに

## ■ ASIS インターナショナル日本支部

ASIS インターナショナル日本支部は次のように積極的な活動を展開しています。

1) 月次セミナーの定期開催
2) セキュリティ専門家（特に在日外国企業のセキュリティ責任者）との情報交換
3) 事業継続計画の専門家との情報交換
4) 公的機関セキュリティ専門家との情報交換

日本支部入会のメリットは次のとおりです。

- 月刊誌「セキュリティ・マネジメント」の購読
- 月刊誌「月刊セキュリティ研究」の購読
- 各種ボランティア活動への参画

このコーナーへのお問い合わせや入会お申込みは
ASIS インターナショナル日本支部　事務局まで

〒101-0021　東京都千代田区外神田 2-2-17
日本保安人事株式会社内
TEL　03-3255-3468　　FAX　03-3258-7630
E-Mail info@asis-japan.org/
www.asis-japan.org