

イベント開催の報告

IW2003 JNSA+JPCERT/CC 共催セミナー

『Security Day ～技術だけでは守れない～』

「Internet Week 2003」が2003年12月2日(火)～5日(金)に社団法人日本ネットワークインフォメーションセンター(JPNIC)主催でパシフィコ横浜会議センターにおいて開催されました。ここで参加団体のイベントの1つとして、特定非営利活動法人日本ネットワークセキュリティ協会(JNSA)と有限責任中間法人JPCERTコーディネーションセンター(JPCERT/CC)が共催で、「Security Day～技術だけでは守れない～」を開催しました。JNSAとJPCERT/CCはこれまで、独立したプログラムでイベントを開催していましたが、Internet Weekで初めて共催しました。両団体にとっても今後更に協力関係を結ぶ上でのエポックメイキングとなる催しとなりました。

今回のプログラムは、2つの基調講演を柱に、JNSAとJPCERT/CCの活動紹介を絡め、最後にBoFで締め括るという構成でした。ここで主なプログラムについてご紹介します。

1. ふたつの基調講演

今回は基調講演として、奈良先端科学技術大学院大学教授・山口英先生とIT関係に詳しい牧野二郎弁護士からお話を頂きました。

まず山口英先生が「セキュリティ管理と高信頼性組織の構築」というテーマで大きな問題提起と考え方が提示されました。この基調講演では、組織のセキュリティ管理担当者が直面している典型的な悩みを考えてみようという切り口で、

1. セキュリティ管理強化の努力を継続的に行っているのに、なぜセキュリティトラブルは減らないのか
2. 発生するトラブルはいつも思いもよらなかったことで発生し、その対応に右往左往してしまうのはなぜか

といった「悩み」や「疑問」に対する考え方を提示するとともに、その中に含まれる課題についての指摘がされました。特に2. に対する対策として「レスポンス力を高めるモデル」を分析してみると、それがかつての日本オリジナルの方法である「力ある技術者から生み出される知見」「経験則」「現場主義」などが重要であり、過去の知恵を現代に生かすことが重要であるという提言がされました。

午後は、牧野二郎弁護士による基調講演「法的立場から見たITセキュリティ」というテーマで、法律の専門家からみたITセキュリティの問題について解説されました。「セキュリティ」の考え方や解釈について、ネットワーク管理者向けのポイントが整理して提示され、専門外だが重要な点について具体的な事例を交えてわかりやすく説明されました。また、今ネットワーク管理者に求められているのは、技術的セキュリティ対策だけではなく、情報セキュリティ全般へ拡大しているという現状を把握できる有用なポイントを掴むことができました。まさに「技術だけでは守れない」ネットワークセキュリティを具体的にわかりやすく解き明かしてくれましたが、今後ともこのようなお互いの専門性をクロスオーバーさせる場が必要であることも痛感したひと時でした。

各々の基調講演に続いて、JNSAのWGと、JPCERT/CCの活動報告が行われました。JPCERT/CCが11月から運用を開始した定点観測システムの紹介、JNSAのWGの中から、ハニーポットWGとセキュリティ被害調査WGなどが紹介され、正規のプログラムは終了しましたが、このあとBoFが開催されました。





2. BoF「眠れない夏、オペレータの戦い」

夜の部は誰でも参加できるBoFとして「眠れない夏、オペレータの戦い」が開催されました。昨夏のCisco IOSの脆弱性やBlaster/Nachiワームの蔓延などを踏まえ、「オペレータにとっての脆弱性情報の流通」をテーマにパネルディスカッション形式で会場の参加者も交えて活発な議論が行なわれました。

- モデレータ 水越一郎氏(JPCERT/CC)
 パネラー (発表順)
 寺田真敏氏(日立/慶應)
 三ツ木絹子氏(MEX)
 白橋明弘氏(ネットワンシステムズ)
 佐藤慶浩氏(日本HP)

モデレータとして水越氏が口火を切り、まずパネラーから問題提起と現状が説明されました。最初は寺田氏が、セキュリティ関連の公開情報を時系列にまとめてWebで公開されている中から、Cisco IOSの脆弱性情報、Blaster/Nachiワームについてまとめた情報を紹介されました。2番目に、三ツ木氏がISPを取り巻く状況の変化と悩みについて率直に語られ、3番目に白橋氏がSIベンダの立場からの思いと現状を話された。脆弱性情報をCERT/CCからのアドバイザリで初めて知るの不安があるので、あらかじめ人員などの体制を準備しておくことができよう公開時期だけでもあらかじめわかっていると対応がしやすい、という提案がされました。最後に、佐藤氏が、脆弱性情報の流通に関して、国際標準などの

策定に関わった立場から、公的な届出機関やISPやSIベンダといった特定の相手に、情報開示を事前にするのが難しい理由について説明がありました。

会場からは、「事前の情報開示は難しいということだが、実現できる可能性はないのか?」といった質問がでました。これに対し、万が一情報が漏れたためにインシデントが発生した場合、「一般ユーザ」の被害に対して損害賠償が請求されると、事前に情報を得て漏らしてしまった「特定ユーザ」が「被害に見合った莫大な金額」を支払わなければならない可能性があること、また情報を出す側も、いわば顧客でもある「特定ユーザ」に対して莫大な損害賠償を請求することは難しいということ、などが障害になっているとの説明がありました。この点については、他の場で行政府も含めて、JNSA、JPCERT/CCなどでの議論が行われており、更に意見交換をし議論を深める必要があると思われる。

朝10時から夜8時までという大変長い「セキュリティ・デイ」でしたが、ほとんどの参加者が最初から最後のBoFまで参加してくださいました。また、会場からの質問も積極的であり、大変有意義な一日であったと思います。参加者からいただいたアンケートの集計結果を見ても大変好評であり、次回Internet Week 2004では、より内容の充実したプログラムを用意したいと考えております。

