

2001 年度 システム技術分科会第 2 回会合 懇談会
テーマ：個人環境とセキュリティ

1. 日時 : 2001 年 10 月 31 日(水) 19:30~21:30
2. 場所 : 神戸ベイシェラトン ホテル&タワーズ 3 階「摩耶」
3. コーディネータ : 長谷川明生 (名古屋大学大型計算機センター) *兼話題提供
久門耕一 (富士通研究所ソフトウェア研究部) *兼話題提供
4. 参加者 : 17 名
5. 討議要旨 :

3 名からテーマに関する各種話題を提供頂き幅広く討議した。

1) 久門氏から個人環境について報告があった。

外部からは Global-address (DHCP で設定)で見える Linux マシンのみで、内部は Private-address で Ethernet, 無線 LAN を構築している。ADSL常時接続にした。性能は 1.5Mbps 程度でほぼ予想通り快適。ところが、平均で 10 件/日(Nimda を考慮するとピークで 300 件/日) のアタックがなされる。内容はポートスキャンして、穴を探しそこに色々なものを仕込んで来る様な手口である。アタック内容のログ採取機構などを仕込んで調査。相手は様々であるが韓国、中国、台湾が多い。曜日、時間などの統計を作成。現地時間で土曜の夜、日曜の午後などが多いと考えられる。また、ウイルスについても、CODE-RED, Nimda などが問題発生の日にきちんと攻撃されてきている。防御をしていなければ、間違いなく感染する。

2) 名古屋大学の長谷川氏から、大学での外部からのアタック状況について報告された。

CODE-RED の時は 33 千件/日だったが、Nimda の時は 23 万件/日と、Nimda の感染力を示すデータが提示された。Nimda の場合には一掃されるのに時間が掛かって居る。

3) 理研の鈴木氏から無線 LAN のセキュリティ問題についての調査報告がなされた。

現状の無線LANのセキュリティは厳密に考えると甘く、セキュリティ機能が 3 つ有るが、プロが盗聴などを試みると簡単にできてしまう。最低でも、3 つのセキュリティ機能を全て実施し、更に SSH を使うなどの工夫が必要との見解が示された。新しい規格も検討されており、今後の動向に注意が必要。

4) 上記 3 項を受け参加者を含めて意見交換を実施した。

- ・ビジターなどの短期滞在者や職員・留学生住居施設へのネットワーク構築が話題となつているところが多いが、セキュリティ対策など問題は多い。
- ・ネットワークは補正予算などで構築しているが維持費が問題である。Firewall、IDS の signature の更新などは必須である。
- ・大学の場合、「卒業学生の id が消されていない」、「管理者なしの linux 機が稼働状態のままとなっている」などのセキュリティ面の問題がある。
- ・まだまだ常時接続はしない事に尽きる。

などの意見が出された。

以上