JANOG43 Meeting 参加レポート

北陸先端科学技術大学院大学
情報科学系 セキュリティ・ネットワーク領域
博士前期課程 1 年
北沢　尭宏

JANOG43 Meeting に参加して

はじめに、JANOG 若者支援プログラム運営委員の方々、JANOG43 Meeting に参加させていただき、誠にありがとうございました。

全体を通しての感想

私が JANOG43 Meeting に参加した目的は、二つある。一つは、ネットワークに関わる研究者としての意識向上のためだ。その理由は、私がネットワークに携わるようになって日が浅いため、自分の立場を認識する必要があると考えたからである。もう一つの目的は、最新技術の動向を知り、私自身の知識の向上させるためである。

実際に、JANOG43 Meeting への参加は私の想像以上のものだった。特に私の印象に残ったプログラムは、「PPP-EXP: ダークネットから見えること」だ。これまで私は、ダークネットによる送信元不明な通信は、全て悪意のある攻撃者からの通信であり、telnet や ssh による遠隔操作を目的としているものばかりだろう、と考えていた。そのため、流れるパケットは TCP の SYN パケットだと考えていた。しかし、公開されたデータでは、SYN-ACK や UDP 通信、ICMP パケットが含まれていたことに非常に驚いた。また、送信元の国ごとに対象とするポートが異なる傾向にあること、またネットワークスキャンした結果を商売にする事業や割り当てされていない IP アドレスからの通信が必ずしも悪意のある攻撃でないことなど、普段接することがないために意識しないことを知ることができて非常に有意義であった。

今回、このプログラムを公聴して私は、ダークネットからの通信内容をハニーポットで観測・解析することで、そのポートを使用するアプリケーションの脆弱性を見つけることにつながるのではないかと考えた。特定の地域でのみ特徴的な内容をもつ悪意のある通信が発生するのであれば、その地域で広く使用されているアプリケーションやネットワーク機器の脆弱性がある可能性が高いと考えられる。もし可能であれば、ダークネットからの通信を利用した脆弱性の早期発見について研究したいと考える。

JANOG、自分に対して思った感想等

今回、JANOG43 Meeting に参加することで、自分が知識不足であることを実感できたことと、自分の興味・関心のある範囲を広められたことが非常に大きな収穫であったと考える。

次回の JANOG Meeting までに自分の持つ知識を深め、参加されているネットワーク技術者と一緒に頷き、質問できるようになりたいと思う。