エグゼクティブサマリ

従来のDDoS攻撃は、マルウェアに感染した大量のPCによるBotnetを悪用し、いっせいに攻撃対象に通信を発生させるものが主流でした。それが2013年頃から、ホームルータやインターネットカメラなどIoT機器の不適切な設定を利用したり、それらの脆弱性を悪用してマルウェアに感染させることによる大規模なDDoS攻撃が観測されるようになりました。

インターネットに接続されるIoT機器の数は今後も大きく増加すると想定され、それらの機器がDDoS攻撃に利用されるのを防ぐことは、安全なインターネットを保つ上でとても重要です。そのような脅威に対応するため、日本では2月1日に総務省、国立研究開発法人情報通信研究機構(NICT)、電気通信事業者により、IoT機器調査と利用者への注意喚起を促す取り組み「NOTICE(National Operation Towards IoT Clean Environment)」が発表されました。

NOTICEでは、NICTがインターネット上でサイバー攻撃に悪用されるおそれのあるIoT機器を調査し、当該機器の情報を電気通信事業者に通知します。通知を受けた電気通信事業者は、当該機器の利用者を特定し、注意喚起を行うことになっています。これは官民が協力して、インターネットに接続されるIoT機器の安全性を高める取り組みであり、IIJもその一員として積極的に参加しています。

「IIR」は、IIJが研究・開発している幅広い技術の紹介を目指しています。私たちが日々のサービス運用から得られる各種データをまとめた「定期観測レポート」と、特定テーマを掘り下げた「フォーカス・リサーチ」から構成されています。

1章の定期観測レポートでは、SOCレポートを取り上げます。IIJのSOCでは、サービスとして提供しているセキュリティ機器のログをはじめ、様々なログを情報分析基盤に集約・分析し、観測した脅威情報を「wizSafe Security Signal」でタイムリーに発信しています。ここでは「wizSafe Security Signal」で発信したレポートのなかから、情報分析基盤を活用して明らかになった特筆すべき3つの活動と、情報分析基盤を活用した機械学習について紹介します。

2章のフォーカス・リサーチ(1)では、IIJの社員がBlack Hat Europe 2018で発表した内容を「ディープラーニングを用いたログ解析による悪性通信の検出」として再構成・掲載しました。特殊な装置やセキュリティ機器を用いるのではなく、一般的なサーバやネットワーク機器のログから、汎用的に脅威を検出できるような仕組みを検討しました。これらの膨大なログは複雑な処理が必要ですが、適切に加工してディープラーニング向けに最適化すれば、有効活用できる可能性があることを確認しています。

3章のフォーカス・リサーチ(2)では、IIJが提供しているメールゲートウェイサービス「IIJセキュアMXサービス」のリニューアルについて紹介します。本サービスは提供開始から10年以上が経過していますが、今もなお契約数が大きく伸びているIIJの代表的なサービスの1つです。とはいえ、10年も経つと利用環境が変化すると同時に、システムも陳腐化し、様々な課題を抱えていました。それらの課題を解決するためのアーキテクチャの見直しや、システムの自社開発という判断など、実際に開発に携わったエンジニアのレポートが参考になれば幸いです。

IIJでは、このような活動を通じて、インターネットの安定性を維持しながら、日々改善・発展させていく努力を続けています。今後も、企業活動のインフラとして最大限にご活用いただけるよう、様々なサービス、ソリューションを提供し続けてまいります。

島上 純一(しまがみ じゅんいち)
IIJ 取締役 CTO。インターネットに魅かれて、1996年9月にIIJ入社。IIJが主導したアジア域内ネットワークA-BoneやIIJのバックボーンネットワークの設計、構築に従事した後、IIJのネットワークサービスを統括。2015年よりCTOとしてネットワーク、クラウド、セキュリティなど技術全般を統括。2017年4月にテレコムサービス協会MVNO委員会の委員長に就任。