エグゼクティブサマリ

東京で二度目のオリンピック・パラリンピック競技大会が開催される2020年。大会に向けた準備が最終段階に入ろうとするなかで飛び込んできたのは、新型コロナウイルスのニュースでした。地球上で人や物の往来がますます活発になった現在、感染症の急速な伝播を防ぐことが非常に困難になっていると、日々の報道を見ていて強く感じます。WHOや各国の政府機関が協力して伝播防止に取り組んでいるにもかかわらず、感染者の数は日に日に増えています。

急速に伝播するのはウイルスによる感染症だけではありません。インターネット上では膨大な情報が猛烈なスピードで流通しており、新型コロナウイルスに関しても様々な情報が私たちの目に入ってきます。それらの情報は必ずしも正確なものばかりではなく、特定の視点に立ったもの、特定の者の利益を代弁したもの、あるいは、故意に受け手を誤認させる悪意を持ったものなど、様々です。情報通信技術が高度に発達した今を生きる私たちは、多様な情報を入手する自由を持つと同時に、膨大な情報の真偽を自ら調べ、考え、行動することが求められていると、今回の出来事を通じてあらためて認識させられました。

「IIR」は、IIJで研究・開発している幅広い技術を紹介しており、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は、サービス提供しているセキュリティ機器のログをはじめ、膨大なログを情報分析基盤で分析し、得られた脅威情報を情報発信サイト「wizSafe Security Signal」でタイムリーに発信しています。本レポートにおいては、2019年の主要なセキュリティトピックのなかからSOCが注目したものをリストアップすると共に、情報分析基盤の活用から明らかになった特筆すべき活動として、Elasticsearchサーバからの情報漏えい、DDoS攻撃、Emotetについて紹介します。いずれもIIJ独自の観測データを交えた解説となっており、興味深く読んでいただけると思います。

2章のフォーカス・リサーチでは、Vol.45に引き続きフォレンジック向けメモリイメージの取得について解説します。前号はLinuxのメモリイメージの取得に関してでしたが、今号はWindowsのメモリイメージの取得についてです。単にメモリイメージを取得するツールの紹介ではなく、メモリイメージの取得時や解析時に注意すべき点を解説します。また、個々のプロセスのダンプを確実に取得する方法も提案します。

3章のフォーカス・リサーチで取り上げたのは、IIJ-II技術研究所が行っている、解析対象への前提知識を必要としないバイナリプログラム解析技術です。プログラム解析技術は統合開発環境に組み込まれ、開発の効率化やバグの削減などに役立っています。一方、マルウェアの疑いのあるプログラムの振る舞いを調べる際など、既に配布された「得体の知れない」バイナリプログラムの解析が必要となる場合があります。本研究では前提知識のないバイナリプログラムでも静的解析が可能な技術を開発しており、ここではその内容を紹介します。

IIJは、このような活動を通し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活用いただけるよう、様々なサービスや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。