エグゼクティブサマリ

この3ヵ月は仮想通貨取引所での仮想通貨の不正流出に関する報道が相次ぎ、世間の注目を集めています。これらの事件の原因は仮想通貨自体にあるわけではないので、これによって様々な可能性を秘めた仮想通貨の利活用に悪い影響が出ないよう注意する必要があるでしょう。

このエグゼクティブサマリを書いている最中に、memcachedのアクセス制限に関する注意喚起が行われました。数日後には、それを悪用して、GitHubに対して1.35Tbpsという過去最大級のDDoS攻撃が発生した、と発表されました。過去にもDNSやNTPなど、トラフィックを増幅する機能を悪用した攻撃手法はありましたが、今回のmemcachedの増幅率は1万を超えるという点で、今までにない破壊力を持っています。このような事象に対してIIJは、他の事業者とも協調して対応していきたいと考えています。

IIRは、IIJで研究・開発している幅広い技術の紹介を目指しており、我々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章では、今号の定期観測レポートとして、SOCレポートを取り上げます。前号でご案内した通り、IIRに掲載していたセキュリティレポートは、より即時性の高いwizSafe Security SignalというWebサイトでの掲載に変更しましたが、年に一度は、定期観測レポートとしてセキュリティを取り上げていきます。今回は、IIJのSOCで独自のセキュリティインテリジェンスを作り出すために刷新した、新しい情報分析基盤を紹介し、この半年のあいだにwizSafe Security Signalで報告した内容から、この情報分析基盤を活用して明らかになった活動について解説します。

2章、3章は、フォーカス・リサーチです。まず2章では、IIJのフルMVNOの取り組みを紹介します。MVNOは名前の通り仮想的な移動通信事業者ですが、自社で保有・運用する機能要素の範囲によって、いろいろな事業モデルがあります。フルMVNOとは、無線アクセス以外の機能要素を自社で保有するMVNOの事業モデルです。多くの設備を自社で保有することにより、今まではMNO（無線アクセスを保有する従来の移動通信事業者）にしかできなかったサービスを、MVNOでも提供できるようになります。そこで、フルMVNOになるとは具体的にどういうことなのか、どのようなことが可能になるのか、といったことを解説します。

3章では、多数のマルチベンダが出力する大量のログを高速で蓄積・検索できるシステムとして、IIJ技術研究所が実装したオープンソースソフトウェア「Hayabusa」について解説します。ネットワークやシステム運用の現場では、ハードウェアやソフトウェアから出力されるログを収集して、統計情報として表示したり、トラブルシュートのために検索する必要があります。セキュリティインシデントに対応する際も、ログの情報は非常に重要です。大規模なシステムにおいては、大量のログを蓄積し、高速で検索する必要があり、それを容易に実現する仕組みとしてHayabusaが開発されました。ここではInterop Tokyoで収集されたShowNetのsyslog実データをもとに行った実験の結果と、Hayabusaの実装・課題などについて紹介します。

IIJ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。今後もお客様の企業活動のインフラとして最大限に活用していただけるよう、様々なサービス及びソリューションを提供し続けていきます。

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。