エグゼクティブサマリ

2017年が始まりました。1月は行く、2月は逃げる、3月は去る、とあわただしく過ぎていく季節になりました。トランプ政権の話題が絶えない中で、スパイ映画さながらの出来事が起きたりして海外から目が離せません。また、一見穏やかに見える国内の政治状況ですが、最近のセキュリティインテリジェンスにまつわる事件は、インターネットにも関係してくる大事なことでもあり、技術論だけで片付けられない事象への対応が増えてくる気がしてなりません。

本レポートは、このような状況の中で、サービスプロバイダとしてのIIJが、インターネットやクラウドの基盤を支え、お客様に安心・安全に利用し続けていただくために継続的に取り組んでいる様々な調査・解析の結果や、技術開発の成果、ならびに、重要な技術情報を定期的にとりまとめ、ご提供するものです。

1章は、過去3 ヵ月間のインターネットセキュリティのサマリーとなりますが、DDoS攻撃についてはサーバを狙ったものが数多く観測される中で収容設備の上流の回線を埋め尽くすような攻撃も増加しています。こうした攻撃は複合的に行われるものが多く、攻撃手法も巧妙になってきていると言えます。また、今回のフォーカスリサーチでは、Ursnifの解析妨害とその回避手法について取り上げました。マルウェアが自分自身の解析を妨害しC&Cサーバに接続するという目的を達成するための巧妙な手法を取り上げ、これを回避する方法について、実例を示しながら解説しています。

2章では、ライブラリOSを取り上げました。OSはコンピュータの進化と共に開発され、非常に高度なものになってきました。また、一方ではソースコードが公開され、学生から研究者が世界レベルの共同作業で開発に参加できるようにもなっています。ライブラリOSはこのようなOSとは少し異なり、カーネルに必要最小限のものだけを残し、それ以外をライブラリの形で提供することにより、柔軟な用途に耐えうるOSの設計を支援するものなのです。本章では、実際に開発に参加している開発者自らが、Linux Kernel Libraryを取り上げてその内容を紹介していますので是非ご覧ください。

プレスリリース等でもお知らせしております通り、昨年発表させていただいた「安全をあたりまえに」をコンセプトとしたブランド「wizSafe」を立ち上げ、セキュリティ事業の強化に取り組んでおります。

これまでIIJでは、セキュリティオペレーションについて通常の運用体制の中に組み込み、技術部門全体で共通の運用技術とし一体として運用して参りました。今後は、これらの運用技術とIIJ独自の解析基盤をベースとしたセキュリティインテリジェンス情報をお客様のシステムを守る観点でも活用していただけるよう、セキュリティオペレーションセンターをリニューアルし、C-SOC サービスなどを通じてお客様に提供させていただくこととなりました。

このような取り組みの一環として、このIIRや各種情報提供手段を通じ、引き続きインターネットの安定性を維持しながら、さらに安心なものにするために「wizSafe」を掲げ、インターネットをより一層良いものにして行く活動に邁進して参ります。

山井 美和（やまい よしかず）

IIJ 常務執行役員 サービス基盤本部長。
1999年6月IIJに入社と同時に株式会社クロスウェイブコミュニケーションズへ出向し、WDM・SONET網構築、広域LANサービスの企画、データセンター建設に従事し、2004年6月に帰任。帰任後は、IIJのサービス運用部門を担当。2016年4月からはインフラ運用部門を加え、IIJの法人ITサービス全般の運用を統括。同時にIIJのデータセンター事業を統括し、国内初の外気冷却を用いたコンテナ型の「松江データセンターパーク」の立ち上げを主導している。

© 2017 Internet Initiative Japan Inc.