

エグゼクティブサマリ

最近、仮想通貨の基礎技術として使われているブロックチェーンについての記事を多く見かけるようになりました。暗号化技術と相まって新たなビジネスや技術の可能性を広げるものだと期待される一方、ランサムウェアによる身代金支払いにビットコインが使われたりと、複雑かつ高度になっていく技術を使うことへの不安が入り混じっていると感じています。インターネットを安心して安全に使うための技術動向についてこれまでも繰り返しご紹介してきましたが、インターネットのインフラだけでなく、社会インフラとしてインターネットを使う上でのセキュリティについての理解を深めていただくために技術情報を提供することによって、こうした不安を払拭していくことも私どもの使命だと考えています。

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章では日々のインシデントや期間中に起きた出来事を中心に、これまでに取り上げた攻撃や事件のその後を追跡し分析しています。相変わらず、AnonymousなどによるDDoS攻撃が続いており、捕鯨問題に関連するところから端を発した直接関係なさそうな官公庁や個人サイトへの攻撃も観測されています。ランサムウェアへの感染による被害拡大が身代金を要求する手口へと巧妙化している現状や、その対処方法について解説することにより、こうした状況への対応の一助になればと考えています。また、暗号に関わる国際的な標準化動向についての解説も加えています。

2章では、ほぼ1年ぶりにメッセージングテクノロジーについて取り上げました。迷惑メールの割合は、一時的な増加はあるものの、ここ数年は総じて減少傾向にあります。技術動向については、DMARCの特徴を詳細に解説しながら、IIJサービスの中から得られた情報から補足説明を加えて解説しています。

3章では、技術トレンドとしてIETFでのTLSの議論を紹介します。同様の技術として長らくSSLが使われてきましたが、2011年から利用禁止が推奨され、TLSへの移行が推奨されています。ただ、TLSが制定されてから約17年、現在主流となっているTLS 1.2が策定されてから既に8年が経過しており、TLS 1.3の策定作業が急ピッチで進んでいます。本章では、TLS 1.2での動作解説を行いながら、最終的には変更となる可能性があります。TLS 1.3で取り込まれる新技術も紹介し、理解を深めていただこうと考えています。

本号を発行する頃には「G7伊勢志摩サミット2016」が終わり、世界中がリオデジャネイロオリンピック・パラリンピック一色になり、その影で社会インフラのセキュリティ対策強化が急ピッチで進んでいると思います。様々なセキュリティ対策を講じる必要性をより強く感じられる今日この頃ですが、インフラ側だけでなく使う側の皆様と一緒に、社会インフラとなったインターネットを守る取り組みを考える上でも、今回の記事は参考になりましたでしょうか。

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も、日々改善し発展させていく努力を続けております。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。