

## エグゼクティブサマリ

我が国では、通信の秘密は憲法で保障されており、IIJのような電気通信事業者、ならびに、それに従事する者は、電気通信事業法において、取り扱う通信の秘密を侵してはならないとされています。一方、電気通信事業を営むうえでは、課金のために顧客の通信履歴を参照したり、パケットを宛先に届けるためにヘッダ情報を参照するなど、通信の秘密を侵して事業を行っています。これらに加えて、迷惑メール対策のフィルタリングやOP25B、児童ポルノブロッキングなど、インターネットを安心してご利用いただくために、私たちISPが常日頃から行っている行為のなかには、通信の秘密に抵触するものもありますが、それらはお客様の同意をいただいていたたり、刑法における違法性阻却の枠組みに沿って慎重に整理がなされています。

そのようななか、4月に政府の知的財産戦略本部が決定した「インターネット上の海賊版サイトに対する緊急対策」において、法制度整備が行われるまでの臨時的かつ緊急的な措置として、特に悪質な海賊版サイトをISPがブロッキングするのは適当であると提言されたことは、私たちISPにとって大きな驚きであり、法律家や消費者団体などからは強い懸念が表明されました。今後、タスクフォースを立ち上げて議論されることになっていますので、注視していきたいと思えます。

IIRは、IIJで研究・開発している技術の幅広い紹介を目指しており、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、特定テーマの掘り下げた「フォーカス・リサーチ」から構成されています。今回は、1章の定期観測レポート、2章のフォーカス・リサーチ(1)ではROCAと呼ばれるRSA暗号アルゴリズムの鍵生成モジュール、3章のフォーカス・リサーチ(2)では電子メールを取り上げています。

1章の前半では、IIJのメールサービスで検知した迷惑メールの受信メールの推移を、2008年から2017年までの500週分について報告すると共に、2017年の特徴的な動きを解説しています。後半では、迷惑メール対策に有効な送信ドメイン認証技術DMARCの普及状況や標準化の動向、更には日本で導入する場合に重要となる法的な取り扱いに関して解説しています。

2章のフォーカス・リサーチ(1)においては、ROCAと呼ばれるRSA暗号アルゴリズムの鍵生成モジュールの実装不備に絡み、プログラムもしくは設計の不具合により、暗号が想定していた安全性を確保できていない事例や、そのような脆弱性を引き起こす要因の分析、更には研究結果が及ぼす今後の影響について報告しています。

3章では、IIJが提供している数百万規模のサービスプロバイダ向け大規模メールシステムの構築や、その運用で蓄積した不正利用対策について紹介しています。メールシステム管理者の業務の多くは、メールシステムの不正利用に起因した対応やそれに付随する障害対応です。そのため、メールシステムに不正利用対策を確実に実装することは、運用管理の負荷軽減や、エンドユーザへの安定的なサービス提供に大きく寄与します。

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おります。今後も、皆様の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。