

## 最近のセキュリティ事件から学ぶこと

株式会社ラック

JSOC チーフエバンジェリスト 兼 担当部長

川口 洋

### 要旨：

インターネットを經由したサービスを提供するうえで欠かせない公開ウェブサービスに対する攻撃の事例を解説する。ログイン機能を提供するサービスを攻撃対象とした不正アクセス(通称：リスト型攻撃)の被害が大きくなっている中、サービス提供者における効果的な対策が少なく、攻撃を防ぐことが難しくなっている。また、ミドルウェアやアプリケーションサーバのようなサービスを構築する上で非常に重要なコンポーネントも攻撃の対象にされている。これらのコンポーネントはウェブサービスを構築する重要なコンポーネントであるにも関わらず、使用されていることが把握されておらず、脆弱性情報が公開されても、対策が取られていない事例が多く存在する。

公開サービスを構築するコンポーネントの脆弱性が攻撃対象となる一方で、メンテナンス経路からの攻撃も多く行われている。サービスをメンテナンスするパソコンがウイルスやマルウェアに感染し、サーバのログイン情報(IP アドレス、ユーザ名、パスワード等)が盗まれ、不正にログインされている。メンテナンス用パソコンの脆弱性管理はサーバそのものの脆弱性管理ほど十分に行われておらず、被害にあう事例も多い。ひとたびメンテナンスに関するログイン情報が盗まれた場合、正規のアカウントでログインされるため発見が難しい。

本講演では上記のような攻撃の事例を紹介し、そのセキュリティ対策について解説する。またセキュリティ対策を推進するための人材育成についての取り組みもあわせて紹介する。