

Topic

平成 23 年 11 月 4 日

80/TCP に対するアクセスの増加について

ワームの感染活動が原因と考えられるアクセスの増加を検知しています。

警察庁では、平成 23 年 10 月 19 日以降、多数の IP アドレスから、80/TCP に対するアクセスの増加を検知しています。(図1)

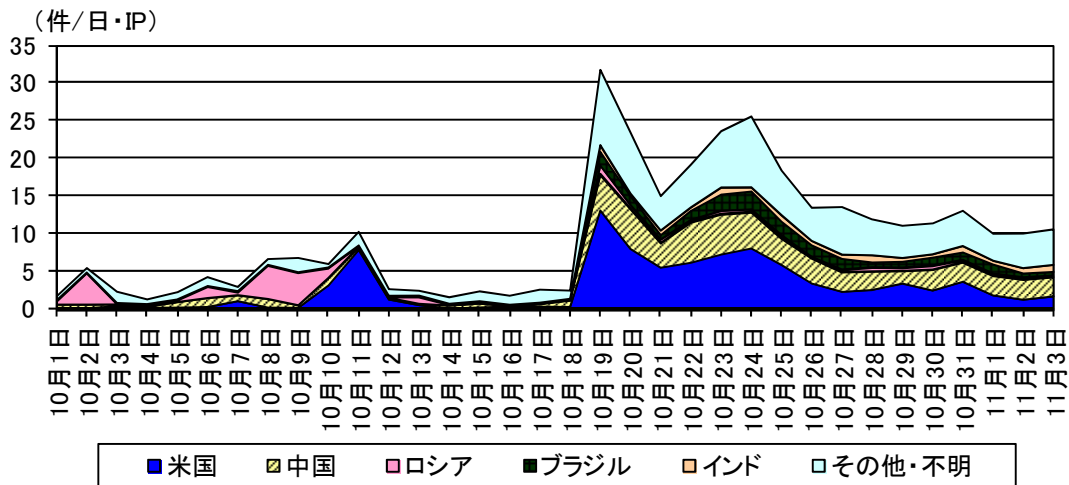


図1 80/TCP に対するアクセス状況

80/TCP に対するアクセス増加の原因の一つに、ワームの感染活動が考えられます。これは、80/TCP を使用し、感染対象を探索するワームが出現しているためです。このワームは、アプリケーションサーバ(クライアントからの要求による、データベース等へのアクセスを管理する機能を持ったサーバソフトウェア)「JBoss」の脆弱性を利用し、感染を広げます。このワームは、さらに悪意のあるプログラムをダウンロードし、被害を拡大させる可能性があります。

先のアプリケーションサーバを導入している場合は、ワームが感染活動に悪用しているとみられる脆弱性が解消された最新のアプリケーションサーバを導入するなどの適切な対策を講じてください。