ダークネットトラフィックの相関分析
Correlation Analysis of darknet traffic

深澤成孝
Hidetaka Fukazawa

＜要旨＞

ダークネットでは，DDoS 攻撃、DNS アンプ攻撃などの大規模な攻撃を行うための事前活動や新しいマルウェアの出現によるスキャン活動などのトラフィックが観測される事例が数多く報告されている．また，近年，官公庁・政府機関・企業などを狙った標的型攻撃や新たな攻撃手法である水飲み場型攻撃などのサイバー攻撃は，今まで以上に高度化・巧妙化している．

このような多様な攻撃が行われているサイバー空間において，早期に攻撃を検知する方法の一つとして，ダークネットに関する研究が数多くされており，ダークネットに届くトラフィックを分析することにより，これから発生しうる攻撃の予兆や大規模感染の予兆などを捉えられる可能性がある．

本論文においては，日本の NICTER と世界の NORSE で観測されるダークネット網のトラフィックデータの相関分析を行い，日本と世界で観測されるダークネットトラフィックに相関関係があることがわかった．

＜Abstract＞

In the darknet, abnormal packet traffic related with prior activity for performing DDoS attacks and DNS amp attack can be observed. Scanning activity by some new malware could be detected also on the darknet. So far many researchers have identified various types of attacks with the analyses of darknet traffic and delivered effective information of detecting an attack at an early stage. They are an offensive omen and an omen of large-scale infection. Especially in recent years, the cyber attacks have been sophisticated, and some of them are called APT (Advanced Persistence Threat) which targets government and related agencies and companies. Further, watering hole attack is known as another type of sophisticated cyber attacks. In order to prevent the above sophisticated cyber attacks, the observation and analysis of traffic on the darknet will be more important than ever before. In this paper, we perform a correlation analysis of traffic data of two different darknet observation systems, NICTER and NORSE. It was found that there is a correlation darknet traffic observed in these systems.