

[ 招待講演 ]

## スレトリサーチの実際と課題

松川博英<sup>†1</sup>

**概要**：近年、サイバー攻撃への対策として「スレトリインテリジェンス」の活用が注目を集めています。データや情報をインテリジェンスに昇華するには、良質なデータの収集とともに、対策すべき脅威に対する能動的なリサーチ活動である「スレトリサーチ」が不可欠です。このスレトリサーチの現場では実際にはどのようなことが行われているのでしょうか？ 似た概念であるインシデント調査やインベスティゲーションとは何が異なるのでしょうか？ 本講演では、情報セキュリティ企業のスレトリサーチャーの立場から、スレトリサーチの実例を紹介するとともに、課題と展望を考えます。

**キーワード**：スレトリサーチ、スレトリインテリジェンス、サイバーセキュリティ

## The Reality of Threat Research and Challenges

Bakuei Matsukawa<sup>†1</sup>

**Abstract**: In recent years, the use of "Threat Intelligence" for a measure against cyber-attack has attracted attention. In order to sublimate data and information to intelligence, it is essential to collect good quality of data together and conducting "Threat Research", which is an active research activity on cyber-threats needed to be addressed. What is the things actually done at the site of the threat research? What is the difference with the similar concepts such as incident handling and investigation? In this lecture, actual examples of the threat research will be introduced to discuss issues and future outlook of threat research from the stand point of threat researcher of information security company.

**Keywords**: Threat Research, Threat Intelligence, Cyber Security

---

<sup>†1</sup> トレンドマイクロ株式会社  
Trend Micro Incorporated.