# インシデント分析センター nicter

㈱情報通信研究機構　ネットワークセキュリティ研究所
サイバーセキュリティ研究室

サイバーセキュリティ研究室では、日々進化を続けるサイバー攻撃を世界規模の大局的な視点で観測・分析し、迅速かつ効果的な対策を実現するため、実践的なサイバーセキュリティの研究開発に取り組んでおり、インシデント分析センターｎｉｃｔｅｒを開発しています。

ｎｉｃｔｅｒ（Network Incident analysis Center for Tactical Emergency Response）は、ネットワーク上でインシデント（セキュリティ事故）を誘発する様々な攻撃への迅速な対応を目指したサイバー攻撃観測・分析・対策システムです。大規模なネットワーク観測システムと、マルウェア*の自動解析システムを融合させ、ネットワークで今まさに起こっている『現状』を俯瞰的に把握し、さらにその『原因』と考えられるマルウェアをリアルタイムに特定します。

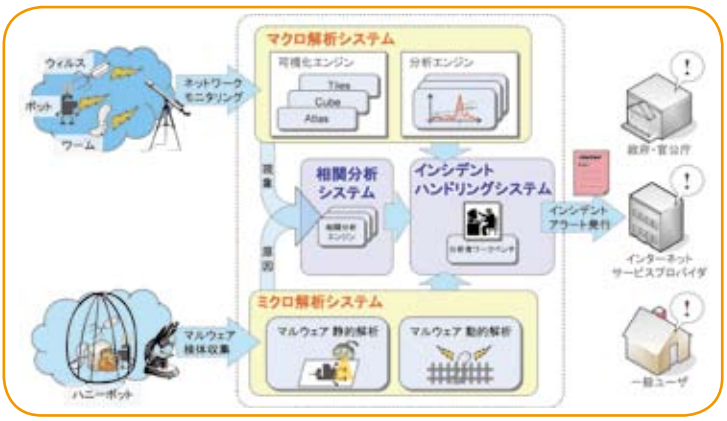


図１．nicterの全体像

*マルウェア：情報漏えいやデータの破壊・改竄、他のコンピュータへの攻撃など、ユーザの望まない不正な活動を行うソフトウェアの総称

ｎｉｃｔｅｒは、未使用のＩＰアドレスブロック（ダークネット）をサイバー攻撃の大規模観測に利用しています。未使用のＩＰアドレスに対しパケットが送信されることは、通常のインターネット利用の範囲においては稀（まれ）ですが、実際にダークネットを観測してみると、相当数のパケットが到着します。これらのパケットの多くは、マルウェアの感染活動など、インターネットで発生している何らかの不正な活動に起因しており、ダークネットに到着するパケットを観測することで、インターネット上の不正な活動の傾向把握が可能になります。

ｎｉｃｔｅｒは、Atlas/Cubeなどの可視化エンジンを備えており、今まさに起こっているサイバー攻撃の状況を視覚的に捉えることが可能です。

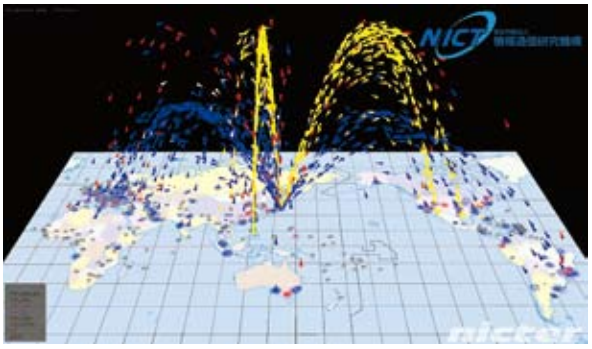


図２．可視化エンジンAtlas

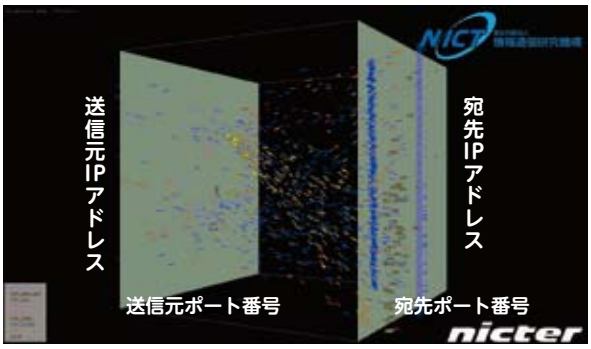


図３．可視化エンジンCube

ｎｉｃｔｅｒの大規模ダークネット観測網で収集している観測情報の一部はＷｅｂで公開しています。サイバー攻撃の大局的な傾向を広く公開することで、情報セキュリティ関連組織や企業・大学の情報セキュリティ管理部門等との情報共有を促進し、我が国のネットワークセキュリティの向上に役立てるとともに、一般ユーザの皆様にサイバー攻撃の状況をお伝えしていきます。公開ＵＲＬは、http://www.nicter.jp/です。

㈱情報通信研究機構ＮＩＣＴは、今後も我が国のネットワークセキュリティの向上に寄与し、国民のネットワーク利用の安心・安全につながるよう取り組んでいきます。