サイバー攻撃の観測情報をWebで公開
ー nicterが収集した情報の利活用を促進 ー

NICTにて研究開発をすすめているnicter（ニクター）（Network Incident analysis Center for Tactical Emergency Response）は、サイバー空間で発生する様々な情報セキュリティ上の脅威を迅速に観測・分析し、有効な対策を導出するための複合的なシステムで、サイバー攻撃*1やマルウェア感染の大局的な傾向をリアルタイムにとらえることができます。昨今、ネットワークセキュリティに対する国民的な関心が高まるにつれて、nicterの収集している観測情報の利活用が期待されていました。

そこで、このたび、NICTは、nicterの大規模ダークネット*2観測網で収集している観測情報（ダークネットトラフィック）の一部をWebで逐次公開することとしました。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: http://www.nicter.jp/ ）

当初、公開する情報は下記のとおりです。

ー ダークネットトラフィックの可視化結果【リアルタイム】
ー ダークネットトラフィックの統計情報【1週間分】
ー ダークネットトラフィックの各種トップ10【1週間分】

今後も、NICTは、nicterWebの掲載情報の充実や安定性向上を進め、真に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。

●nicterWebの表示画面

*1　サイバー攻撃
コンピュータネットワークで構成されるサイバー空間において、不正アクセスやマルウェア感染等により、国家や企業などに損害を与えようとする行為。近年、米国では「サイバー空間」を陸、海、空、宇宙に次ぐ空間として、国家安全保障上重要視するなど、世界中においてサイバー攻撃に対する対策が急務となっている。今回、NICTが観測するサイバー攻撃は、主にPCの脆弱性などを探索するためのスキャン行為であり、サイバー空間全般にある攻撃すべてを網羅しているものではない。

*2　ダークネット
インターネット上で到達可能かつ未使用のIPアドレス空間のことを指す。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）であるが、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することが分かる。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いる。そのため、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る。