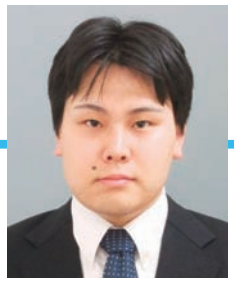
セキュリティ対策を支える技術
―インシデント分析センターNICTERとその利活用―



国立研究開発法人情報通信研究機構　サイバーセキュリティ研究所
サイバーセキュリティ研究室 主任研究員　笠間（かさま）　貴弘（たかひろ）

1. はじめに

「彼を知り己を知れば百戦殆うからず」は孫子の有名な格言である。サイバーセキュリティの世界ではどうしても後手に回りがちな防御側で「百戦殆うからず」を達成するのは相当困難だが、今起きているサイバー攻撃の観測・分析を通じて彼（攻撃側）の現状を知ることは、サイバーセキュリティ対策において大きな役割を果たしていることは間違いない。

本稿では、インターネット上で発生しているサイバー攻撃の現状を把握するために、情報通信研究機構サイバーセキュリティ研究室において13年以上に渡り実施しているNICTERプロジェクトの紹介と、そこで観測・分析された最新の攻撃活動の状況を解説する。

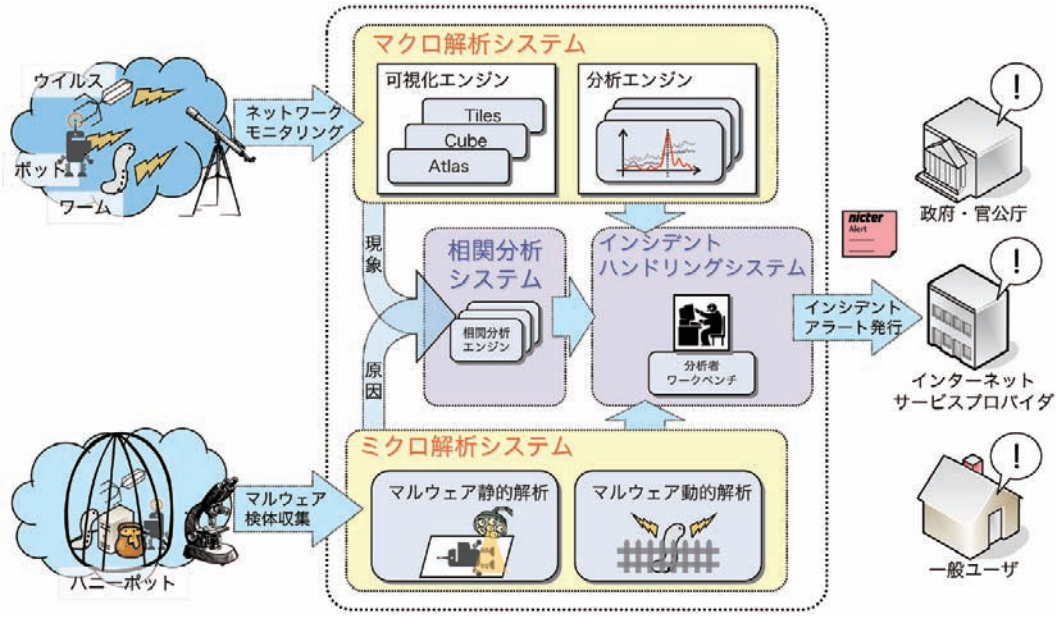
2. インシデント分析センター NICTER

NICTER（Network Incident analysis Center for Tactical Emergency Response）はリモート感染型マルウェア（いわゆるワームタイプのマルウェア）の世界的な活動傾向をリアルタイムに把握し、それらに起因したサイバー攻撃の発見と原因究明・対策導出を目的として、2005年に研究開発をスタートした。2005年というと、2003年にBlasterワームが登場し、その後SasserワームやSQL Slammerといった世界規模での大規模感染につながったワームが次々と登場してきた時期であり、それらの感染状況を正確に把握するということが当初の目的の一つであった。

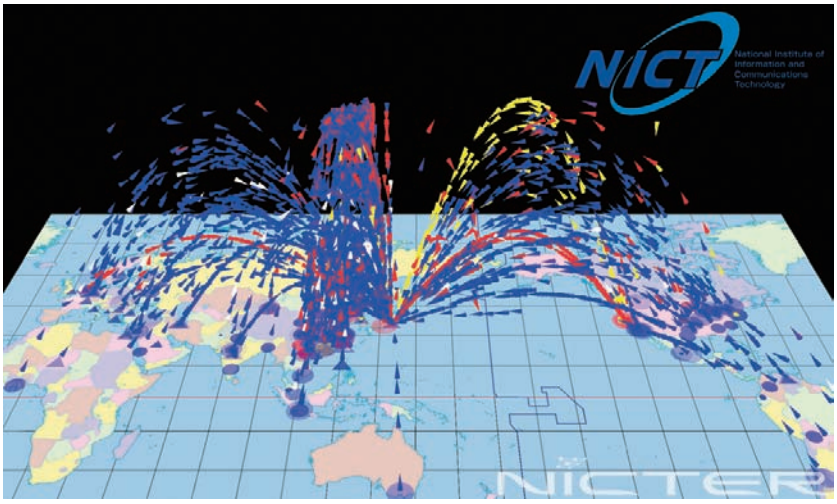
NICTERは大きく分けて、マクロ解析システム、ミクロ解析システム、相関分析システム、インシデントハンドリングシステムの4つのサブシステムから構成されている（**図1**参照）。まずはこれらのサブシステムの概要を紹介する。

2.1　マクロ解析システム

マクロ解析システムでは、国内外の複数拠点に設置したセンサを通じて、「未使用のIPアドレス」宛ての通信を観測している。本来、未使用のIPアドレスに対して通信が発生することはないが、後述するように実際には非常に多くのパケットがインターネットから未使用のIPアドレス宛に届いている。これらの大部分はリモート感染型のマルウェアが次の攻撃対象を探すためのスキャンによるものであり、未使用のIPアドレス（以下、ダークネットと呼ぶ）を観測し、得られたパケットを分析することによって、インターネット上におけるセキュリティインシデントの一大要因となっているマル



■図1.　NICTERの全体概要図



■図2.　Atlasによる攻撃可視化

ウェアの活動傾向を把握することができる。我々は2005年に約1万6千アドレスのダークネットから観測を開始し、その後連携組織を増やしながら、現時点では十数か国に約30万アドレスのダークネット観測網を構築・運用している。

マクロ解析システムには、観測されたパケットを分析する複数のエンジンが含まれており、例えばトラフィック量の急増などのインシデントの可能性の高いイベントを自動的に検出する。また、観測されたパケットを可視化エンジンによってリアルタイムにアニメーション表示することで、オペレータが視覚的に観測状況を把握できるようにし「人間の気づきの力」を活用できる仕組みを備えている。例えばAtlas（**図2**参照）は観測されたパケットの1つ1つについて送信元IPアドレスの情報から緯度経度を割り出し、パケットが観測された様子を地図空間上にアニメーション表示する可視化エンジンである。色でパケットの種別（TCPやUDPなど）を表し、軌道の高さで宛先ポート番号を表すなどの工夫によって、地理的な攻撃分布状況だけでなく狙われているサービスなども直感的に把握できる。

NICTERのダークネット観測データの一部はWebサイト（NICTERWEB[1]）で一般公開しており、誰でも最新の観測傾向を知ることができる。

2.2　ミクロ解析システム

ミクロ解析システムでは、ハニーポットと呼ばれる囮サーバやWebクローラなどを利用し、実際のマルウェアの収集を行う。収集されたマルウェアは複数の解析エンジンによって自動的に解析が行われ、解析結果が蓄積される。特に、ミクロ解析システムでは大量に収集するマルウェア検体を効率的に解析するため、解析環境内で実際にマルウェアを動作させ、その際に観測されたAPI呼出しやネットワークアクセスを観測することで、マルウェアの機能や特徴を明らかにする動的解析システムの構築に力を入れている。我々はシステムの並列化によって、現在1日に7,000検体以上を解析可能なシステムを構築している。

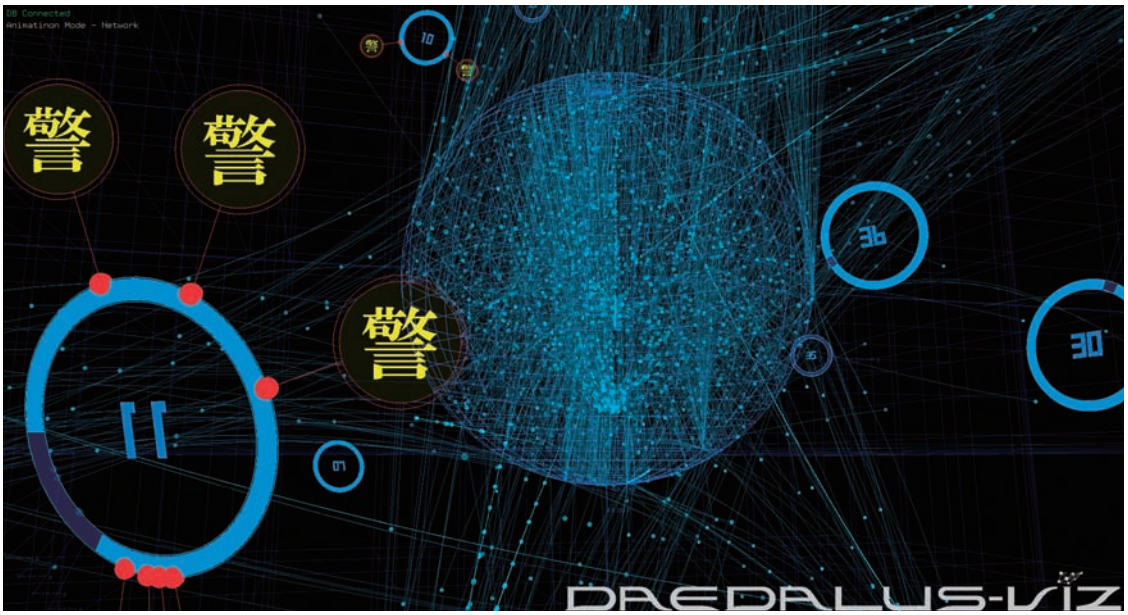
2.3　相関分析システム

相関分析システムはマクロ解析システムで観測されたマルウェア感染端末からのスキャン活動をプロファイリングし、同様にミクロ解析システムで解析したマルウェアのスキャンのプロファイルと突合することで、類似のスキャンプロファイルを検知する。つまり、実際にインターネット上で観測された攻撃活動の原因となっているマルウェアを見つけ出すシステムである。

例えば、2016年に発見されIoTデバイスへの大規模感染を引き起こしたMiraiマルウェアは、スキャンパケットの生成時に、TCPヘッダのシーケンス番号を攻撃先のIPアドレスの値に設定するという特徴があり、このようなマルウェアの作りに依存した特徴を相関分析システムで捉えることで各マルウェアの感染規模推定などにつなげている。なお、Miraiはソースコードがインターネット上で公開され、Miraiのソースコードを基に開発されたと見られるマルウェアが多数発生しており、前述の特徴を持つスキャンはMiraiに限定されない。

2.4　インシデントハンドリングシステム

インシデントハンドリングシステムは、上記3つのシステム



■図3．DAEDALUSアラートの可視化

の出力を集約・蓄積し、インシデント発生時のデータ管理や再現等を実現する。また、我々は大規模ダークネット観測を基にしたアラートシステムDAEDALUS（ダイダロス）を開発・運用している（**図3**参照）。DAEDALUSは組織内のマルウェア感染端末が行うスキャン活動などをダークネットで観測した際に、当該組織に対し自動的にアラート送信を行うシステムである。DAEDALUSの機能はアラート送信ができる対象が主にワームタイプのマルウェア感染となっており限定的ではあるものの、未使用IPアドレスへの通信をトリガーとすることで確度の高いアラート提供が可能となっている。DAEDALUSの仕組みは技術移転という形で民間企業にライセンスされ製品・サービス化されているほか、JLIS（地方公共団体情報システム機構）が窓口となり、現在は全国約600の地方公共団体に対して無償でアラート提供を行うなど様々な活用がなされている。

3．最新のサイバー攻撃観測状況

本章では、NICTERの観測状況を報告することで、最新のサイバー攻撃の状況について解説する。

3.1　NICTER年間観測統計

表に我々の2005年から2016年までの観測結果の統計を示す。

我々はより多くの攻撃活動を観測できるように、ダークネットの規模を拡大してきたが、単純な総観測パケット数は観測対象のダークネットの規模に大きく影響されるため、表の右端に観測IPアドレス数で正規化した数（IPアドレス1つ当たりで観測された年間のパケット数）を示している。正規化した値を見ると、ダークネットで観測されるパケット数は2005年から基本的に増加傾向を示し続けていることが分かる。つまり、ドライブ・バイ・ダウンロード攻撃に代表されるWeb媒介型攻撃の流行や、スマートフォンなどのモバイル環境を狙った攻撃、システムの脆弱性ではなく人を狙ったソーシャルエンジンニアリングなど、日々新たな攻撃が登場してくる一方で、従来からのリモート感染型攻撃はその数を減らすことはなく、継続した被害を出し続けているということである。ICTの進歩に応じてサイバーセキュリティを取り巻く状況は日々刻々と変化しており、その中で我々の注意

■表．NICTER年間観測統計

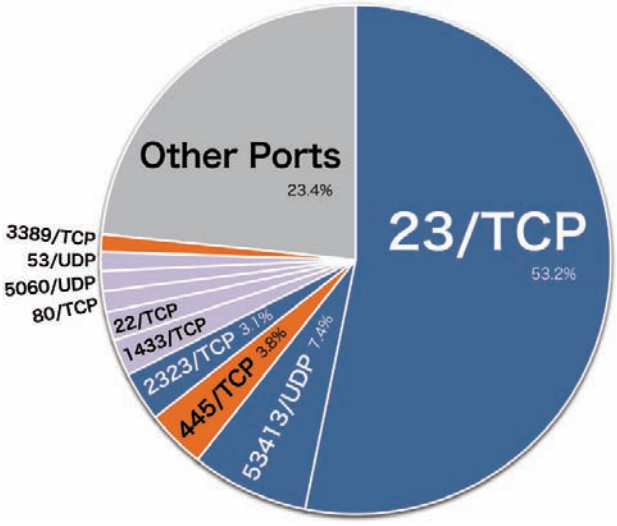
年	年間総観測パケット数	観測IPアドレス数	1 IPアドレス当たりの年間総観測パケット数
2005	約 3.1億	約1.6万	19,066
2006	約 8.1億	約10万	17,231
2007	約19.9億	約10万	19,118
2008	約22.9億	約12万	22,710
2009	約35.7億	約12万	36,190
2010	約56.5億	約12万	50,128
2011	約45.4億	約12万	40,654
2012	約77.8億	約19万	53,085
2013	約128.8億	約21万	63,655
2014	約256.6億	約24万	115,323
2015	約545.1億	約28万	213,523
2016	約1281億	約30万	469,104

も新たな脅威に優先して向けられてしまう傾向があるが、一つの重要な点として、従来からの脅威もその多くが決して消え去ったわけではないことは認識しておく必要がある。

3.2　IoTデバイスの大量感染

また、表を見ると、特に2013年以降は正規化した観測パケット数が毎年倍近い増加を示していることが分かる。この増加は、前述したMiraiに代表される主にLinux系OSが動作しているWebカメラやWiFiルータ、デジタルビデオレコーダといった機器（ここでは一まとめにIoTデバイスと呼ぶこととする）を狙ったマルウェアの感染被害が拡大した影響によるものである。図4に2016年の年間観測パケットをプロトコル及び宛先ポート番号別に集計した上位10個を示す。

図を見ると、23/TCP（Telnet）宛てのパケットが全体の半数を超えており、これは上記のIoTデバイスの中には、初期設定でTelnetが動作しており、さらにデフォルトのID/Passが設定された不適切な設定状態のままインターネットに接続されているものが多数存在するため、それを狙って感染を拡げようと試みるマルウェアが多く発生している影響である。2016年では、IoTデバイスを狙った攻撃（図4中の青色の部分）は全パケットの約6割以上となっており、現状のリモート感染型マルウェアの感染分布として多数を占めていることが分かる。こうした機器は一般的なPCなどと異なり、アンチウイルスの導入が難しいケースや、セキュリティパッチの適用といった適切な管理が為されていないケースがあり、今後増々増加していくであろう、IoTデバイスのセキュリティ対策は重要な課題になっている。



■図4．攻撃対象別のパケット数統計（2016年）

3.3　日本における大量感染の事例

2017年に発生した日本における攻撃事例として、ルータ製品を狙った大量感染事例を紹介する。

2017年10月31日頃、NICTERにおいて23/TCPに対してMiraiの特徴を持つパケットを送信するホスト数の増加を確認した。これらのパケットの送信元の多くが日本国内のIPアドレスであったことが分かり、ICT-ISACやJPCERT/CCなどの国内関連組織と情報共有を行い、更なる調査を進めたところ、それら送信元IPアドレスの多くで、某メーカ製のブロードバンドルータが動作している状況が判明した。また、一部機器のUPnP（Universal Plug and Play）用インタフェース（52869/TCP）がインターネット側からアクセス可能であり、NICTERの観測でも52869/TCP宛ての通信が観測されていたため、ハニーポットを用いて52869/TCP宛ての通信を分析した結果、Realtek SDKのMiniigdサービスにおけるコマンドインジェクションの脆弱性（CVE-2014-8361）を攻撃する通信であることが分かった。当該攻撃が成功した場合には、Mirai亜種がダウンロードされ感染する。

つまり、日本国内のIPアドレスを送信元とする23/TCPへのスキャンの増加は、上記の52869/TCP宛ての攻撃に対して脆弱な特定の機器が国内に多数存在し、その結果としてそれらの機器がMirai亜種に感染し、23/TCPへのスキャン活動を行っていた可能性が高いことが明らかになった。この調査結果は、メーカにも適切に連絡し情報共有した上で、観測レポート[2]として公開した。

4．まとめと今後の課題

インターネット上で発生するサイバー攻撃を観測・分析するためのNICTERプロジェクトの取組みを紹介し、最近の観測状況について解説した。リモート感染型マルウェアの被害はIoTデバイスの増加に伴いますます増加しており、日本でも大量感染の事例が発生している状況が明らかになっている。有効性のあるセキュリティ対策を検討する上では、実際のサイバー攻撃をきちんと観測し、実データを基に議論ができる仕組みを構築することが重要であり、我々は今後も継続した研究開発を進めていく。

参考文献

[1]“NICTERWEB,” http://www.nicter.jp/
[2]“NICTER観測レポート　ルータ製品の脆弱性を悪用して感染を広げるMirai亜種に関する活動（2017-12-19），” http://www.nicter.jp/report/2017-01_mirai_52869_37215.pdf