特集

マルウェア

編集にあたって

寺田真敏（(株)日立製作所）　菊池浩明（東海大学）

15,317,951

さて，何の数字であろうか？

本特集「ボット対策プロジェクト 『サイバークリーンセンター』からみた国内のマルウェア対策」で取り上げたサイバークリーンセンターで 2007 年から 3 年間に収集したマルウェア(ボット)検体の総数である．換算すると，サイバークリーンセンターでは，6 秒[☆1] に 1 個，ボットを収集していたことになる．ボットは，有害なプログラムの総称であるマルウェアの一種で，外部の指令者からの命令を待ち，その命令に従って不正な動作をするプログラムである．

☆1 3 年 x 365 日 x 24 時間 x 60 分 x 60 秒（=94,608,000 秒）÷ 15,317,951 検体 =6.17 秒 / 検体

7日間

この数値は，マルウェア配布サイトや配布サイトへの誘導などに利用されるドメイン名（malware.example.ipsj.or.jp のような形式で表記する名称のこと）の平均利用期間である．本特集「マルウェア観察日記 (2)」で取り上げた調査結果によると，作成されてから実際に利用されるまではわずか 2 日間であるという．開いて，攻撃して，すぐに撤退する．数と早さに圧倒されてしまうばかりである．

ここ数年の間に，ワーム，スパイウェア，ボット，フィッシング，標的型攻撃など数多くのセキュリティ用語が生まれている．情報システムが直面する脅威は格段に広がり，被害の形態も様相を変えてきている．そこで，この特集では，有害なプログラムの総称であるマルウェアを対象に，マルウェア対策へのさまざまな取り組みを取り上げることとした．敵が多様ならば守り方も多様にせざるを得まい．さまざまな視点から，現状を報告・議論いただくことで，マルウェア対策の今後を展望するきっかけにしたい．

本特集では，大きく 5 つの構成とした．

「マルウェアって？」では，用語を整理するために，マルウェアの歴史，マルウェアに含まれる，攻撃コード，ウイルス，ワーム，スパイウェア，アドウェアなどについて解説する．この特集を企画して分かったことは，専門家でさえボットに感染したコンピュータを指すのに「ボット」，「ボット感染ホスト」，「ゾンビ」とまちまちな呼び方をしているということである．

「マルウェア観察日記（1）—静かに進む OS への浸食—」，「マルウェア観察日記 (2) —サービスとして提供される攻撃—」，「標的型メールがやってきた」では，対策の前線にいる研究者／運用者の視点からマルウェアの挙動について紹介する．やや専門的な技術や用語が使われているが，マルウェア研究者の日常の雰囲気が伝わるよう，あえてそのままとした．

「マルウェアと戦う技術」では，技術の変遷と，これからのマルウェア対策に向けた技術について展望する．日常的に利用しているアンチウイルスソフトで用いられている技術の原理を分かりやすく解説している．

「サイバークリーンセンターからみた国内のマルウェア対策」，「研究用データセットを用いたマルウェア対策研究人材育成ワークショップ」，「ナレッジマネジメントツールによるマルウェア挙動の見える化」，「機械語命令列の類似性に基づく自動マルウェア分類システム」，「MWS Cup 2009」は，2008 年からサイバークリーンセンター運営委員会と情報処理学会との共催で開始したマルウェア対策研究人材育成ワークショップについての取り組みを中心にまとめたものである．

本ワークショップは，サイバークリーンセンターの約 100 台のハニーポットで収集した 2 年間分のマルウェアから研究用の共通データセットを作成して，ネットワーク専門家やマルウェア解析の専門家が束になって解析を加える試みである．入力データが共通なので，各研究の優劣が明確に出る．特に，MWS Cup は共通の入力データを与えて，マルウェア種別や振舞いの推測精度を競うコンテストなので，どの研究グループも本気になった．ここで発表された多くの研究の中から，代表的なものを選び，一般向けに書き換えていただいた．マルウェア対策の最前線の熱さを感じていただきたい．

「マルウェア対策に向けた国際連携」では，インシデントに対応する組織や自社製品の脆弱性に対応する製品開発組織の活動を解説している．国内でのマルウェア対策研究の土壌を，アジア，グローバルに展開することができれば，広く奥行きの深い国際連携の実現が期待できよう．さらには，被害抑止に関する国際連携がより効率的で，実効性の高いものとなっていくことを願って，特集のまとめとした．

執筆をお願いした方は，いずれも，マルウェア対策に関する研究開発のみならず，実務部門でも非常に多忙を極められている方々ばかりであり，今回の機会に執筆いただいたことにこの場を借りて深く感謝申し上げる．

本特集がきっかけとなって，マルウェアに関する理解が深まることを望んでいる．また，実効性の高い対策のためには，技術のみならず，各組織の持ち味を活かした連携のあり方についても議論を広げることが必須である．ぜひ，皆の力を結束して，我々の利用するインターネットを安心で安全な環境にしようではないか！

最後に本特集を組むことができたのも「マルウェア対策研究人材育成ワークショップ」という国内でのマルウェア対策研究の取り組みを開始できたことにつきる．本ワークショップを実現するにあたり，企画段階からご協力をいただいた NTTPC コミュニケーションズの小山覚氏，実行段階で取りまとめていただいた北陸先端科学技術大学院大学の篠田陽一教授，研究用の共通データセット準備にあたり多大なる支援をいただいたサイバークリーンセンター関係各位，ならびに，ご協力をいただいた関係組織の皆様にお礼申し上げます．

（平成 22 年 1 月 31 日）