2011 年 9 月 14 日
株式会社日立製作所
KDDI 株式会社
独立行政法人情報通信研究機構

ユーザの PC に潜む未知の不正プログラムを発見・駆除する「マルウェア対策ユーザサポートシステム」を開発 ～システムの有効性をフィールド検証する実証実験を実施～

株式会社日立製作所（以下「日立」、執行役社長：中西宏明）および KDDI 株式会社（以下「KDDI」、代表取締役社長：田中孝司）は、コンピュータセキュリティ対策の分野において、ユーザ PC に侵入した未知の不正プログラム（以下「マルウェア*1」）を発見・駆除する技術の研究を行い、独立行政法人情報通信研究機構（以下「NICT」、理事長：宮原秀夫）が開発したインシデント分析センター nicter*2 のミクロ解析システム*3 と協調動作する「マルウェア対策ユーザサポートシステム」を開発しました。

本システムは、ユーザ PC の負荷を抑えながら、既知/未知を問わずマルウェアを効率的に発見でき、短時間で簡易的な駆除を行うことが可能となります。これにより、日々大量に発生する新規マルウェアへの対応が難しくなりつつあった従来のウイルス対策ソフトウェアを補完することが期待できます。このたび、本システムの有効性を検証するため、日立と KDDI は NICT と共同で、2011 年 9 月 15 日より学校法人を対象に、NICT の nicter ミクロ解析システムを活用した実証実験を行います。

本研究開発は NICT からの委託研究*4 として日立と KDDI が実施しており、日立が主体となり要素技術の開発を行い、KDDI がシステム構築や実証実験の準備を行っています。

1.研究開発の背景

今日、数千から数万に上る未知のマルウェアが日々生み出されています。さらに、それらのマルウェアは自己防衛機能*5 を備えていたり、ゼロデイ攻撃*6 を行うなど、巧妙化・高度化を続けています。そのため、既知のマルウェアの実行コード*7 や攻撃パターンの情報を利用して検知・駆除*8 する従来のウイルス対策ソフトウェア*9 では、新たに生まれ続ける未知のマルウェアに十分に対応することが難しくなりつつあります。

本研究は、ユーザ PC に侵入した未知のマルウェアを効率的に検知・駆除するシステムを開発し、従来のウイルス対策ソフトウェアの機能を補完することを目的としています。

2.今回の成果

マルウェア対策ユーザサポートシステムでは、今回新たに開発したクライアントエージェント*10 と呼ばれるソフトウェアにより、ユーザ PC 内部からマルウェアと疑われる実行コードを探し出し、nicter ミクロ解析システムと協調動作して、その実行コードの内部挙動や外部との通信を解析します。解析の結果、実行コードをマルウェアと判定した場合、解析結果を利用してマルウェアを簡易的に駆除するプログラムを自動生成し、ユーザ PC に配布、駆除処理を行います。これにより、ユーザ PC の負荷を抑えつつ、既知/未知を問わずマルウェアを効率的に発見し、短時間で駆除する仕組みを実現しました。

本システムの動作の詳細は、〈別紙1〉「マルウェア対策ユーザサポートシステム」の動作イメージをご参照ください。

3.実証実験の内容

マルウェア対策ユーザサポートシステムの有効性をフィールド検証するため、下記の学校法人の学生・教職員に、前述のクライアントエージェントがインストールされたPCを配布し、PCでの通常作業に影響を与えずに長期間安定して動作することや、マルウェアが PC に侵入した場合に検知・駆除が適切に行われること等を検証します。

【協力いただく学校法人】

〇玉川大学（東京都町田市）
〇宮城教育大学（仙台市青葉区）
〇鳴門教育大学（徳島県鳴門市）
〇日本コンピュータ専門学校（大阪市東淀川区）
〇大阪情報コンピュータ専門学校（大阪市天王寺区）

【実施期間】

2011 年 9 月 15 日～12 月 31 日

4.添付資料

〈別紙1〉「マルウェア対策ユーザサポートシステム」の動作イメージ
〈別紙2〉 用語 解説

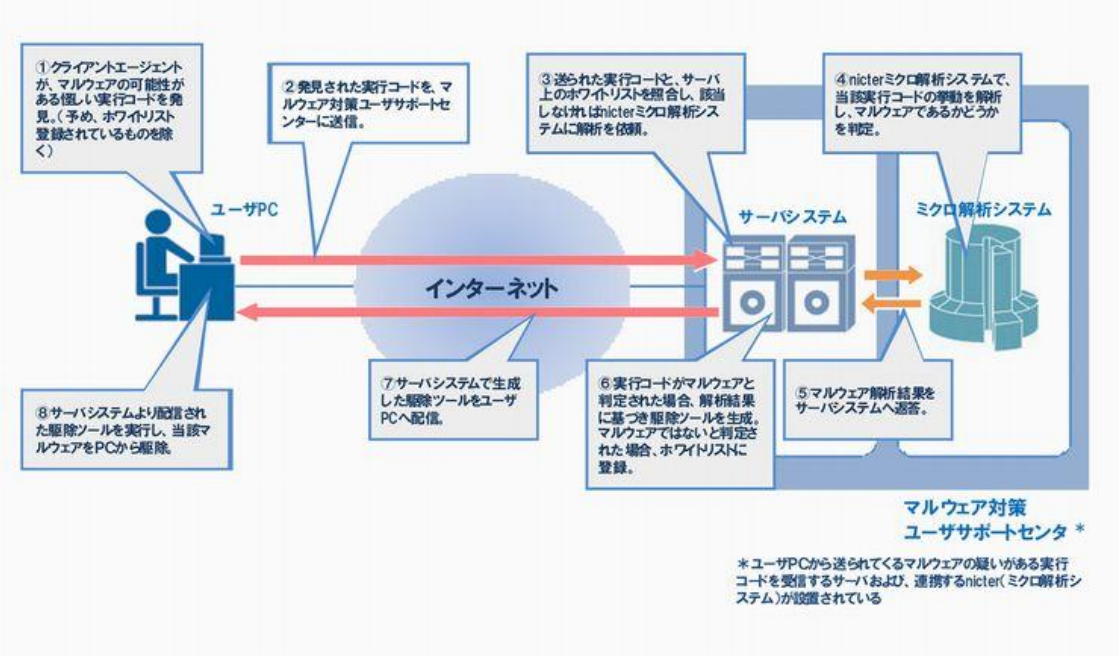
5.本件に関するお客様からのお問い合わせ先

日立：
情報・通信システム社 セキュリティ・トレーサビリティ事業部
事業企画部（担当 ： 赤羽、木村）
TEL : 044-549-1627 (ダイヤルイン)
E-Mail:info-sec@ml.itg.hitachi.co.jp

KDDI：
ソリューション推進本部 ソリューション 3 部
E-Mail：mw-inq@kddi.com

NICT：
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（担当：井上、衛藤）
TEL：042-327-6826 FAX：042-327-7458
E-mail: nicter-pub@ml.nict.go.jp

〈別紙１〉



「マルウェア対策ユーザサポートシステム」の動作イメージ

〈別紙２〉

◆用語 解説◆

＊1 マルウェア

ウイルス、ワーム、ボット、スパイウェア等、情報漏えいやデータ破壊、他のコンピュータへの感染等の有害な活動を行うソフトウェアの総称で、「悪の～」という意味を持つ接頭語の「mal～」とソフトウェアの「ware」を組み合せた造語。

＊2 nicter

Network Incident analysis Center for Tactical Emergency Response の略称。インターネット上で発生する様々なセキュリティ上の脅威を迅速に把握し、有効な対策を導出するための複合的システムで、ネットワーク攻撃の観測やマルウェアの収集等によって得られた情報を分析し、その原因を究明する。

＊3 ミクロ解析システム

nicter のサブシステムの一つで、マルウェアの完全自動解析システム。外部システムから入力された実行コード等を隔離環境の中で動作させ、数分のオーダでその動作を解析し、解析結果をデータベースに蓄積するとともに収集元の外部システムへ返信する。

＊4 委託研究

本研究開発は NICT からの委託研究「マルウェア対策ユーザサポートシステムの研究開発」として 2009 年より日立と KDDI が実施している。日立が主体となり要素技術の開発等を行い、KDDI がシステム構築や実証実験の準備を進め、NICT の nicter ミクロ解析システムを活用して実証実験を行う。

＊5 自己防衛機能

PC に侵入したマルウェアが、ウイルス対策ソフトウェア（＊9）による検知・駆除を回避するために、ファイル構造を暗号化したり、OS を改ざんする機能。

＊6 ゼロデイ攻撃

OS やアプリケーションソフトウェアにセキュリティ上の脆弱性が発見された際に、ソフトウェアベンダ等による脆弱性の修正コードが公開されるよりも前に、その脆弱性を悪用して行われる攻撃。修正コードが公表された日を 1 日目とみなし、それ以前（ゼロまたはマイナスデイ）に攻撃が行われることからこう呼ばれる。

＊7 実行コード

PC 上で動作する、実行形式のプログラム。Windows®では PE(Portable Executable)などが該当する。

※Windows は、米国 Microsoft Corporation の、米国、日本およびその他の国における登録商標です。

＊8 駆除

マルウェアが発見された際に、その活動を無効化するとともに、マルウェアが生成・改ざんしたレジストリ・ファイルなどを、削除・修復し、PC をマルウェア感染前の状態に復旧する動作。

＊9 ウイルス対策ソフトウェア

マルウェアを PC から検知、駆除するソフトウェア。PC 内に常駐し、ウイルス等の特徴を記録したデータファイル（「パターンファイル」または「定義ファイル」「シグネチャ」と呼ばれる）と、PC 内部でやり取りされるデータを比較し合致した場合は駆除や隔離（ファイルをアクセスできない領域へ移動）

を行う製品が多い。

＊10　クライアントエージェント

ユーザPC上に常駐し、PC内部に不審な実行コードが存在する場合に、本システムのユーザサポートセンタに実行コードを送信し、マルウェアであるか否かの解析を依頼する。また、ユーザサポートセンタ側で、当該実行コードがマルウェアと判定された場合は、サーバから配信されてくる駆除ツールを受信・実行し、マルウェアを駆除する。

以上