報道発表

- **ネットワーク攻撃分析と不正プログラム自動解析の最先端技術**
  －Interop Tokyo 2007においてインシデント分析システム“nicter”を実証運用－
- **平成19年6月6日**

独立行政法人情報通信研究機構（理事長代行：田中栄一、以下NICT）は、平成19年6月11日から15日にかけて幕張メッセで開催されるネットワーク分野の世界最大規模の総合イベントInterop Tokyo 2007（＊1）に、NICT が開発したセキュリティインシデント（＊2）対策技術“nicter（＊3）”を出展し、実証的運用を公開（6月13日から15日）します。この技術は、ネットワーク攻撃のリアルタイム分析・可視化技術や不正プログラム（マルウェア＊4）の自動解析等を可能にした最先端の研究成果を基にしています。こうした開発成果により、インシデントの事前対策や迅速な事後対応が可能となり、より安心・安全な情報通信社会の実現が期待できます。

＜背景＞

近年、ウイルスやワーム、ボットといったマルウェアの感染や、それに伴う情報漏えい、Webサービスに対する妨害行為などのセキュリティインシデントが多発し、安心・安全な情報通信社会を構築するうえで、大きな課題となっています。NICTでは、こうしたセキュリティインシデントの早期検知、原因究明、対策法の導出等を目的とした、インシデント分析システムnicterの研究開発を推進してきました。特に、近年のサイバー攻撃の増加・多様化が見られる中で、従来からの分析者の知見や経験に基づく半手動型の解析が困難となってきており、膨大なセキュリティログから攻撃を自動的に分析する技術や、攻撃の状況を分析者に分かりやすく提示する可視化技術、多様なマルウェアにも対応可能で、自動解析を高精度で行うなどの技術開発が切望されていました。

＜開発成果・実証運用の公開＞

NICTでは、ネットワーク上で観測・検知した攻撃をリアルタイムで自動分析・可視化する従来無かった新しい技術を確立し、それをnicterで実現しました。また、マルウェアの検体1つを5分程度で自動解析し、その構造、挙動、感染の仕組み等を明らかにする技術も確立しました。

今回はこれらnicterの分析・解析技術を、ネットワーク分野における世界最大規模の総合イベントであるInterop Tokyo 2007の中核を担うネットワークShowNet（＊5）に導入し、ShowNetに対するネットワーク攻撃をリアルタイムで分析・可視化、そしてShowNetで収集されたマルウェアを自動解析するなどの実証運用を公開します。解析したマルウェアの情報は、ShowNet全体を管理するNOC（Network Operation Center）によって有効利用される予定です。

＜今後の展望＞

今後は、上記ネットワーク攻撃分析技術とマルウェア解析技術とを融合させ、インシデントに対する有効な対策の導出を含む統合的なインシデント対策技術の確立に取り組みます。

＜広報問い合わせ＞
総合企画部 広報室
栗原 則幸
Tel：042-327-6923
Fax：042-327-7587

＜本件に関する　問い合わせ先 ＞
情報通信セキュリティ研究センター
インシデント対策グループ
井上大介　吉岡克成
Tel: 042-327-6225（代表）
Fax: 042-327-6640

補足資料1

【用語解説】

*1 Interop Tokyo 2007:

例年15万人を超える参加者を集め、300社あまりの出展社が最新のネットワーク機器やソリューションを展示し、同時に多数の講演やコンファレンス等が開催される、ネットワーク分野における世界最大規模のイベントです。

参考:Interop Tokyo 2007 http://www.interop.jp/

*2 セキュリティインシデント:

企業や大学等の情報通信ネットワークにおける情報漏えいやデータ改ざん、Webサービスの妨害などの情報セキュリティに関する事故・事象を意味します。近年のインシデントの例としては、Winnyを悪用した不正プログラムによる情報漏えいや、特定の企業や国家の運営するWebサイトへのサービス妨害攻撃などがあります。

*3 “nicter”:

nicter (Network Incident analysis Center for Tactical Emergency Response) はインターネット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なシステムです。ネットワーク攻撃の観測や不正プログラムの収集などによって得られた情報を分析し、その原因を究明します。

*4 マルウェア:

コンピュータウイルス、ワーム、ボット、スパイウェアなど、情報漏えいやデータ破壊、他のコンピュータへの感染などの有害な活動を行うソフトウェアの総称です。「mal-」=「悪の」という接頭辞とソフトウェアの「ware」を組み合わせた造語となっています。マルウェアは近年、多様化かつ高度化する傾向にあり、セキュリティインシデントの有力な原因の1つと考えられています。

*5 ShowNet:

国内外のネットワークベンダが世界最先端のネットワーク機器を結集して構築する、Interopの心臓部ともいえる展示会場全体のネットワークです。

参考: http://www.interop.jp/shownet/index.html

補足資料2

“nicter”の解説

NICT 情報通信セキュリティ研究センター インシデント対策グループでは、インターネットで時々刻々発生しているセキュリティインシデントへの有効な対策を打ち出すため、インシデント分析システムnicter(Network Incident analysis Center for Tactical Emergency Response)の研究開発を進めています。
以下の図に示すとおり、nicterは、4つのサブシステムから構成されています。

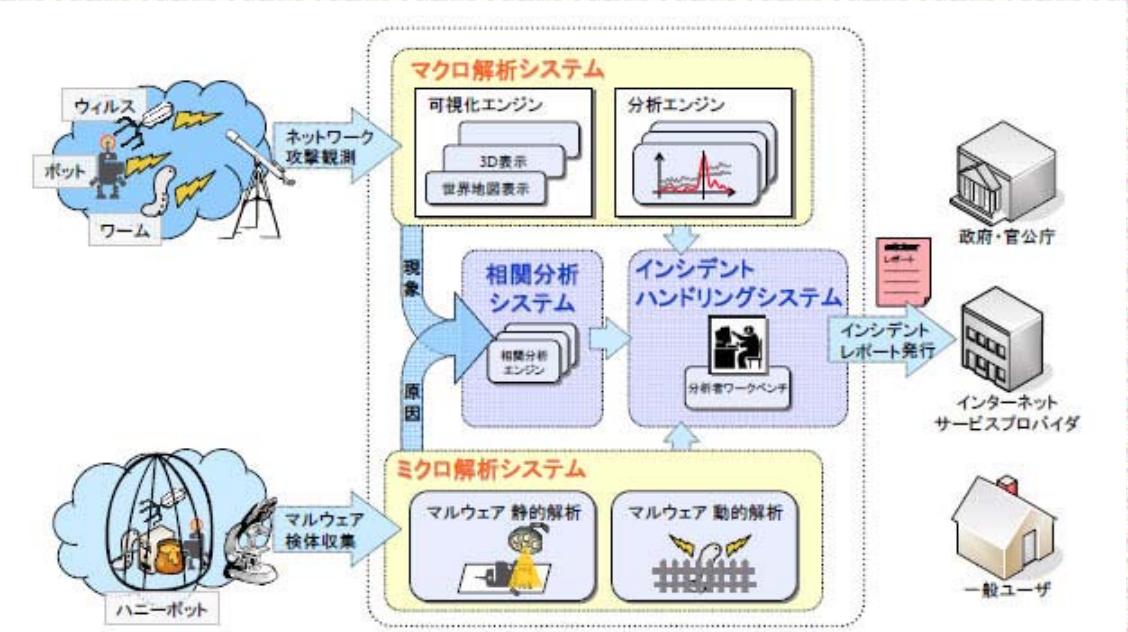
・マクロ解析システム
広域ネットワークを観測し、ネットワーク攻撃をリアルタイム自動分析することで、新たな攻撃の発見や、インシデントの予兆を捉えます。

・ミクロ解析システム
ハニーポット等により、インシデントの原因となっているマルウェアそのものを捕捉し、自動的に解析を行います。

・マクロ-ミクロ相関分析システム
マクロ解析システムによって検知された新たな攻撃やインシデントの予兆と、ミクロ解析システムで解析されたマルウェアの相関を調べることで、ネットワーク上で起こっている現象とその原因を結びつけます。

・インシデントハンドリングシステム
上記の3つのシステムから得られた分析結果を集約・管理するともに、分析者に対するインターフェイスを提供します。また、分析者がインシデントレポートを作成するための補助的な役割も果たします。

なお、Interop Tokyo 2007のShowNetでは、nicterのマクロ解析システム内の分析エンジンや可視化エンジンを用いてネットワーク攻撃の分析を行います。また、ミクロ解析システム内のマルウェア解析技術を用いて、ShowNet内で捕捉されたマルウェアの解析を行います。



nicterの全体像