

平成18年12月21日

報道関係各位

日本電気株式会社
株式会社ラック

データマイニングを活用した新しい情報セキュリティ監視技術を開発

～サイバー攻撃の予兆やコンピュータ上の不審行動を自動的に検出～

日本電気株式会社（本社：東京都港区、代表取締役執行役員社長：矢野 薫、以下NEC）および株式会社ラック（本社：東京都港区、代表取締役社長：三輪信雄、以下ラック）は、大量データの解析を通じて価値ある情報を見つけ出すデータマイニング技術の適用により、サーバへの攻撃を予測的に監視できる高度な情報セキュリティ監視サービスを実現する技術や、コンピュータ上の不審行動分析のための作業効率を飛躍的に改善する技術を開発し、実際のデータを使ってその有効性を実証することに成功しました。

このたびの技術により、個人情報や機密情報の漏えいやデータの改ざんを引き起こし、場合によってはデータベースを乗っ取ってしまうSQLインジェクション（注1）等のサイバー攻撃や、組織内部での情報犯罪など、近年脅威が高まっている情報セキュリティの問題に対して有効な新しいサービスが実現できます。

実証実験は、NECのデータマイニング技術とラックのセキュリティノウハウを組み合わせることにより、実際のWebアクセスログやコンピュータのイベントログ（注2）の中から、セキュリティ上の犯罪行為を自動検出できることを確認する目的で行われました。その主な成果は以下の通りです。

- (1) Webサーバに蓄積された膨大なアクセスログの情報から異常なふるまいを自動検出。その結果、従来は困難であったSQLインジェクション攻撃の予兆を捉えたことを確認。本ケースでは被害発生の22時間前に予兆を捕捉できました。

(2) コンピュータに記録されたイベントログの中で通常のパターンから外れている部分に高いスコアをつけることにより、実際のなりすましを検出することに成功。本ケースでは、スコアの高い上位 1.5%の中に犯罪行為を見つけ出しました。

近年、SQLインジェクション攻撃などの外部からの脅威や、内部統制に関する法整備が進む一方で組織内部での情報犯罪が増加する状況を背景に、これらの事象の発生を監視し、発生時には迅速に対処するサービスへの要求が高まっています。その一方で、サーバへの攻撃や内部犯罪の手口が巧妙かつ多様化しているため、次々に発生する未知の事象を処理しきれていないのが現状です。そのため、IDS(侵入検知システム)をすり抜けたSQLインジェクション攻撃に対する有効な防御方法は無く、被害発生後に事後分析を行うにとどまっていました。また、内部の情報犯罪対策も定期的にログを統計処理して確認する程度が一般的であり、情報犯罪の証拠を効率的に検出できる新技術の出現が待ち望まれていました。

このたび開発した技術の一つは、時系列データの変化点を迅速に検出するNECのマイニングエンジン「ChangeFinder」を適用したものです。Webサーバへアクセスするトラフィック量を分析し、急激に変化が起こったところでアラームを出すことにより未知の攻撃(注3)の始まりを検出できるため、SQLインジェクション攻撃の被害を未然に防ぐサービスの提供が可能となります。マイニング技術によって、予め一定値を超えた場合に発するいわゆるしきい値ベースの監視よりも、早期に攻撃の予兆を検出することが可能になります。

またもう一つの技術は、ログをスコアリングし、異常行動に高いスコアを与えるマイニングエンジン「AccessTracer」を適用したもので、PCのイベントログの中から、内部の情報犯罪につながる不審行為の箇所を効率よく絞り込めます。

NECとラックは今後、今回の成果を活かし、データマイニング技術を適用した新たなセキュリティサービスの提供を目標に、更なる実証実験を進めていく予定です。

以上

(注1) SQLインジェクション攻撃：

データベースサーバに蓄積されたデータを外部から直接改ざんしたり、不正に取得することを目的に、データベースを操作するための言語であるSQLの一部を外部から投入する攻撃のこと。

(注2) イベントログ

コンピュータ上のアプリケーションやハードウェアで発生した事象を管理するWindowsオペレーティングシステム特有の仕組み、もしくは事象の記録のこと。

(注3) 未知の攻撃

予め定義したパターンとの照合によって攻撃を検知する、いわゆるシグネチャベースの検出が困難な攻撃。

※「ChangeFinder」、「AccessTracer」はNECの登録商標です。

■NECデータマイニング技術センターについて

NECは、平成17年12月に「データマイニング技術センター」を設立し、大量なデータを効率的に分析し、価値ある知識の発見や未来予測に役立つデータマイニング技術の適用を拡大し、さまざまな分野への貢献を目指しています。データマイニング技術センターでは、独自の異常検出技術やテキストマイニング技術などを活用したソリューションの企画、サービスビジネスモデルの検討、データマイニング技術の顧客システムへの組み込みおよび適用支援、先端的なデータマイニング技術の研究開発を行っています。

■株式会社ラックについて

株式会社ラックは、いち早くネットワーク社会の到来を予測して1986年9月3日に設立されました。ネットワークセキュリティソリューション分野でのリーディングカンパニーとして、「データベースセキュリティ研究所(DBSL)」、「コンピュータセキュリティ研究所(CSL)」にてセキュリティに関する情報を日々、蓄積・分析・検証を行い、リモート監視センターJSOCにて顧客システムの24時間365日のセキュ

リティ監視・分析を行っています。また、先進のセキュリティテクノロジーを、セキュアネットサービス事業とシステムインテグレーション事業が提供するサービスに付加し、官公庁・企業・団体等の顧客にセキュリティソリューションサービスを提供しています。

■コンピュータセキュリティ研究所（CSL）について

コンピュータセキュリティ研究所（CSL）は、コンピュータセキュリティに関するわが国における最先端の研究機関です。最新かつ多彩な知識を持つセキュリティアナリストたちが、新しい脅威や効果的な対策についての専門的な研究を進めています。その対象も、最新の脅威に対する情報収集・調査から、防御や検査、監視の方法まで幅広い領域に及びます。さらに実際の攻撃手口を用いた実証実験も行っており、防御と攻撃の2つの側面からラックならではのナレッジを蓄積。米国の後追いではなく、日本語環境での特異点にも精通しており、コンピュータセキュリティ研究所が発するCSLレポートの信頼性は国内最高と業界で認知されています。

<本件に関するお客様からのお問い合わせ先>

NEC 研究企画部 企画戦略グループ

<http://www.sw.nec.co.jp/contact/>

株式会社ラック SNS 営業本部 池田

電話： (03) 5537-2610

<本件に関する報道関係からのお問い合わせ先>

NEC コーポレートコミュニケーション部 志村

電話： (03) 3798-6511

E-mail: s-shimura@ak.jp.nec.com

株式会社ラック 管理本部広報室 綱川

電話： (03) 5537-2600

E-mail: pr@lac.co.jp