平成 28 年９月１日

各位

会 社 名　株　式　会　社　ラ　ッ　ク
代表者名　代表取締役社長　髙　梨　輝　彦
（JASDAQ・コード番号：３８５７）
問合せ先　ＩＲ広報室長　岩　﨑　　勝
電　　話　０３－６７５７－０１０７

ラック、大規模標的型攻撃事案への迅速な対応に向け、端末情報収集・解析ツールを開発
～本日創刊の情報誌「CYBER GRID JOURNAL Vol.1」に、技術概要を掲載～

株式会社ラック（本社：東京都千代田区、代表取締役社長：髙梨 輝彦、以下ラック）は、大規模な標的型攻撃事案への緊急対応サービス「サイバー119」の対応強化を目指したツール「インシデント対応ツール（仮）」について、このたび基本的な機能部分が完成しましたので発表します。「インシデント対応ツール（仮）」は、標的型攻撃の脅威にさらされた組織の端末情報を収集・解析するためのツールで、ラックの研究開発部門であるサイバー・グリッド・ジャパンを中心に開発を進めてきました。その機能概要と開発背景に関しては、サイバー・グリッド・ジャパンが本日公開した情報誌「CYBER GRID JOURNAL Vol.1」（創刊号）に掲載しています。

ラックが運営する「サイバー119」は、年間350件を超える緊急対応を実施しています。これらの対応を通じ、標的型攻撃を受けた多くの組織には遠隔操作ウイルスのような高度に作り込まれた不正なソフトウェアが仕込まれてしまい、攻撃の被害は企業ネットワークの深部にまで及んでいることを確認しています。

攻撃者は、狙い定めた企業への侵入にひとたび成功すると、攻撃の痕跡を隠蔽しながら、内部での感染拡大や情報収集、情報持ち出し等の活動を継続します。場合によっては、グループ関係組織や取引先にまで攻撃が波及することも確認しています。このような高度な攻撃を受けた場合、インターネットとの境界で不審な外部通信を監視することに加えて、組織内の端末から必要な情報を収集した上で総合的に解析し、脅威の発見とその対処、原因調査、被害拡大の防止を行うことが求められます。

しかし、実際の緊急対応では、ほとんどの組織で端末の情報を収集できる仕組みが導入されていないため、脅威の発見が遅れて事案の収束に時間がかかるケースが多くあります。

ラックは、このような大規模な標的型攻撃事案への緊急対応を強化するため、これまでの当社の豊富な経験を活用した新たな端末情報収集・解析ツール「インシデント対応ツール（仮）」の開発に着手し、このたび基本的な機能部分の実装を完了しました。今後はいくつかの組織で検証を行って機能改善を図る方針です。本年末を目処に緊急対応現場での本格的な活用を開始し、より迅速かつ的確な事案対応を実現してまいります。

端末情報収集・解析ツール「インシデント対応ツール（仮）」の特徴

要件	説明
自動実行プログラムの精査	OS起動時など、自動的に起動されるプログラムの状況をフォレンジック調査の観点で深い分析を可能にするとともに、コンピューターウイルスと侵害パソコンの迅速かつ正確な特定、事実解明を行うことができる。過去のインシデント対応で得た知見を活用して痕跡チェックや脅威検知を迅速に実現できるようにする。
検知後の調査分析	組織全体の包括的な分析をベースとし、特定のパソコンで発見した不正な事象の精査からそのパソコン以外の影響範囲や脅威の関連性について一連での分析ができるようにする。ログを受け取った後でも被害組織から追加でログが届くことを想定し、分析できるようにする。
被害組織の環境に合わせたログ取得	ログ取得の際は、被害組織の負担をできるだけ少なくする。それにより、システム環境や突発的な事情によるログ取得漏れの状況を極力なくす仕組みにする。
複数パソコンを対象にしたタイムライン解析	ウイルス感染後の組織内の横断的侵害について、手口の解明を従来よりもスムーズにするため、フォレンジック調査の肝とも言えるタイムライン解析を単体のパソコンだけでなく、複数台も対象にして追跡調査が行えるようにする。

端末情報収集・解析ツール「インシデント対応ツール（仮）」については、開発に至った背景や概要について、本日公開の情報誌「CYBER GRID JOURNAL Vol.1」で取り上げていますので、ご覧ください。

「CYBER GRID JOURNAL Vol.1」
http://www.lac.co.jp/security/report/2016/09/01_cgjournal_01.html

ラックは、より複雑化・巧妙化・大規模化するサイバー攻撃に対し、被害をより最小限に抑制するための支援を行うべく、引き続き研究開発活動に取り組んでまいります。

以上

【 株式会社ラックについて 】　（http://www.lac.co.jp/）

ラックは、1986年にシステム開発事業で創業、多くの実績を誇る「金融系の基盤システム開発」「マーケティング・オートメーション支援」「ビッグデータ・アナリティクス」を始め、社会の基盤システムの開発を行っています。1995年にはいち早く情報セキュリティ事業を開始し、現在ではサイバーセキュリティ分野のリーディングカンパニーとして、官公庁・企業・団体等のお客様に業界屈指のセキュリティ技術を駆使した、先端のITトータルソリューションサービスを提供しています。2016年には、米フロスト＆サリバンより、「セキュリティ監視」「脆弱性診断」「セキュリティ事故対応」「セキュリティコンサルティング」などが高く評価され、昨年に続き２年連続で「2016 ジャパン マネージドセキュリティサービス プロバイダーオブザイヤー」を受賞しています。

この件に関するお問い合わせ

■ 掲載記事のお問合せ先には、こちらをご紹介ください。
株式会社ラック
Tel： 03-6757-0113（営業）　E-mail： sales@lac.co.jp
■ 本件に関する取材のご要望は、こちらにご連絡ください。
株式会社ラック　IR広報室　広報担当
Tel: 03-6757-0107（広報部門）、03-6757-0130
E-mail: pr@lac.co.jp　　Twitter： @lac_security
Facebook： https://www.facebook.com/Little.eArth.Corp/
