平成 25 年 12 月 4 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　理事ＩＲ広報部長　白　石　通　紀
電　　話　０３－６７５７－０１０７

ラック、巧妙で悪質なサイバー攻撃に対応するため、『標的型攻撃対策支援サービス』を拡充 ～米 FireEye 社製品を活用し、攻撃を正確に早期発見することで、企業の安全確保を支援～

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、日本の企業や団体に的を絞り行われる巧妙で悪質な「標的型攻撃」や「水飲み場型攻撃＊」などのサイバー攻撃への対応のため、当社が提供する「標的型攻撃対策支援サービス」のメニューを拡充し、悪質な不正プログラム検知で定評のある米 FireEye 社製品（以下、FireEye）を採用した「FireEye 分析支援サービス」を本日より提供開始します。

近年、日本の企業や政府機関等に狙いを定めたサイバー攻撃は高度に巧妙化し、大きな脅威になっています。私たちラックの緊急対応サービス「サイバー119」の出動要請件数も年々増加しており、2012 年は約 250 件出動し、事故対応支援と再発防止対策を実施しました。さらに、本年８月に出動した事案のサイバー攻撃手法は、「水飲み場型攻撃」と呼ばれる、特定または不特定ユーザが Web サイトを閲覧した際に不正なプログラム（コンピュータウイルスなど）を感染させる罠が仕込まれていました。加えて、マイクロソフト社の Internet Explorer の未知の脆弱性が悪用されるなど、最新の更新プログラムを入れ、ウイルス対策ソフトを使用しても、対応できないものでした。

▼日本における水飲み場型攻撃に関する注意喚起と対策方法（2013 年 10 月 9 日）
http://www.lac.co.jp/security/alert/2013/10/09_alert_01.html

今回新たに追加拡充された「FireEye 分析支援サービス」は、ウイルスや不正通信の検知に効果を発揮する FireEye をより有効的に活用し、脅威の正確な実態把握を行います。FireEye が検知して発するアラートをラックが有する優れた分析技術を用いて、脅威の内容、被害実態、影響範囲をご報告します。攻撃の早期発見と正確な実態把握が可能となり、お客様は適切な対策を迅速に施すことが可能となります。FireEye は、仮想のネットワークで不審なプログラムを動かして不正かを判断するため、未知の脅威も高精度に検知します。しかし、利用者には高度なセキュリティ知識と分析能力が求められ、「どのような攻撃なのか?」、「どのような被害があるのか?」、 「自社の環境ではどのような影響があるのか?」など、自社での対応が困難なことが課題でした。ラックは、FireEye 社が日本法人を設立する以前の 2011 年より同社と連携し、日本におけるサイバー攻撃対策を行ってきました。約 2 年にわたる対応実績とノウハウを基に、「FireEye 分析支援サービス」を開発しました。

■「FireEye 分析支援サービス」の主な特徴

・FireEye の機能を最大件に引き出し、より有効活用を実現
・FireEye のアラート内容を正確に理解することで、的確な対応が可能
・FireEye が検知し、発覚した事故に基づいて、全体の脅威を把握
・FireEye の機能を補完する付加サービスを提供

ラックは、本サービスを提供することで、企業、政府機関等のサイバー攻撃対策を支援します。また、日本最大級のセキュリティ監視センターJSOC（ジェイソック）では、FireEye の自社運用が困難な組織への支援策として、2014 年春からセキュリティ監視サービス（MSS：マネージドセキュリティサービス）における FireEye 対応を提供予定です。ラックは引き続き、日本の組織をサイバー攻撃から防衛するためのサービスを提供し続けていきます。

本サービスの正式リリースに対して、米 FireEye 社 Vice President JAPAN/APAC Douglas Schultz（ダグラス・シュルツ）様よりエンドースメントをいただいておりますので、ご紹介をいたします。

【米 FireEye, Inc. Douglas Schultz 様】

ファイア・アイは、LAC 様が新たに「FireEye 分析支援サービス」を開始することを心より歓迎いたします。FireEye の製品が特に強みをもつ、未知のマルウェアや攻撃の検知情報に基づき、LAC 様が脅威の内容や被害実態、影響範囲について分析を行い、お客様にいち早く脅威情報をお伝えすると言うことは、企業のセキュリティ防衛の面で非常に有効であると確信しております。 是非多くのお客様でこのような分析支援サービスを活用し、セキュリティ向上にお役立て頂ければ幸いです。

FireEye, Inc. Vice President JAPAN/APAC Douglas Schultz

▼以下のページでも、「FireEye 分析支援サービス」の情報をご覧いただけます。

http://www.lac.co.jp//service/incident/fireeye_analysis.html

＊）「水飲み場型攻撃（watering hole attack）」とは

水飲み場に集まる動物を狙う猛獣の攻撃になぞらえ、攻撃対象とするユーザが普段アクセスする Web サイト（水飲み場）にコンピュータウイルスを埋め込み、サイトを閲覧しただけでコンピュータウイルスに感染するような罠を仕掛ける攻撃方法です。巨大なポータルサイトのような不特定多数が訪問するサイトに限らず、特定の関心事や組織・業界関係者が訪問する Web サイトも、攻撃対象者を絞り込むための狩り場として狙われています。

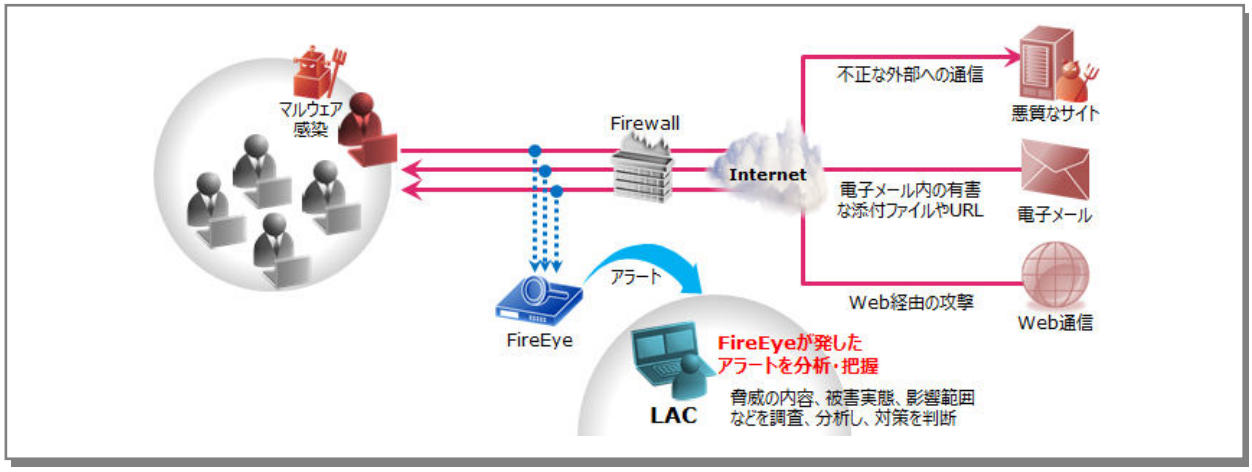
（サービス詳細）

■「FireEye 分析支援サービス」の内容

FireEye は、従来のシグネチャベースの攻撃検知手法に加え、製品内に自動設定された強力な仮想テスト環境で脅威の分析を行うシグネチャレスの検出も行います。Web、電子メールなどに対する保護を統合することにより、標的型攻撃の検知、未知のマルウェアの検出、ゼロデイ攻撃の抑止に貢献します。

今回の「FireEye 分析支援サービス」は、FireEye が検出した脅威アラートから、脅威の度合い、脆

弱性の特定、お客様の環境における影響内容などを分析し、対策支援を提案します。FireEye の機能をより有効活用することで、脅威の実態を正確に把握することができ、お客様は的確な対策を早期に施すことが可能となります。



項目	概要
アラート内容の確認	FireEye により発せられるアラート内容を確認し、誤検知、脅威の度合いなどを調査。必要に応じて安全が確認できるまでの対応を提案。
詳細分析	影響範囲の確認と、脅威の詳細内容及び対象となる脆弱性の特定を行い、必要となる対応を提案。

■「FireEye 分析支援サービス」の主な特徴

・FireEye をより有効活用します

ラックが有する高度なバックドア通信解析やマルウェア動的解析技術によって、「そのマルウェアは本当に危険なのか?」、「その通信は本当にマルウェアによる不正な行為なのか?」といった判断を行います。誤検知を排除することで FireEye の運用をより有効的に行うことができます。

・アラート内容を正確に理解することで、的確な対応が可能

例えば、大きな被害をもたらすことのないマルウェアに対し、標的型攻撃対策のような大掛かりな対応を行うことは不効率であり、影響が軽微な場合はアンインストールで対応するなど、的確な判断が可能です。

・発覚した事故に基づいて、全体の脅威を把握

攻撃の有無を確認するだけではなく、その事実から「マルウェアの挙動内容の確認」、「対象となる脆弱性」などを確認し、組織内全体への影響度を把握することが可能です。

・FireEye 社製品の機能を補完する独自サービス

Proxy ログ解析、Exploit コード解析といったような独自の調査手法を用いて、FireEye 社製品単体では得られない総合的な調査結果を導きます。

■ **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、1995 年にいち早くセキュリティ事業を開始。2012 年４月にグループの合併により、株式会社ラックとして新たにスタート。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、豊富な実績を誇る「脆弱性 診断サービス」、日本最大級の「セキュリティ監視センターJSOC」による 24 時間 365 日のセキュリティ監視・分析サービス、情報漏えい事故などの緊急対応・支援をする「サイバー119」の提供をはじめ、金融機関向け基盤システム開発で培った「システム開発」など、官公庁・企業・団体等のお客様に IT トータルソリューションサービスを提供しています。

【お客様からのお問い合わせ先】	【報道機関からのお問い合わせ先】
株式会社ラック　営業担当 Tel: 03-6757-0113　E-mail: sales@lac.co.jp http://www.lac.co.jp/contact/index.html	株式会社ラック　広報担当 Tel: 03-6757-0130　E-mail: pr@lac.co.jp

以上